THE WORLD BANK
IBRD • IDA | WORLD BANK GROUP

Combatting Cybercrime

Tools and Capacity Building for Emerging Economies


DIANA
DOCTORAIR
Experiencing Massager Shop
体感型
マッサージ器
専門店

Combatting Cybercrime

Tools and Capacity Building for Emerging Economies

Some Rights Reserved

This work is a co-publication of The World Bank and the United Nations. The findings, interpretations, and conclusions expressed in this work do not necessarily reflect the views of The World Bank, its Board of Executive Directors, or the governments they represent, or those of the United Nations. The World Bank and the United Nations do not guarantee the accuracy of the data included in this work. The boundaries, colors, denominations, and other information shown on any map in this work do not imply any judgment on the part of The World Bank or the United Nations concerning the legal status of any territory or the endorsement or acceptance of such boundaries.

Nothing herein shall constitute or be considered to be a limitation upon or waiver of the privileges and immunities of The World Bank or the United Nations, all of which are specifically reserved.

Rights & Permission

1818 H Street, NW, Washington, D.C., 20433
Telephone: 202-473-1000; Internet: www.worldbank.org

Acknowledgments

This Toolkit was developed under a project, *Combating Cybercrime: Tools and Capacity Building for Emerging Economies* (Project), financed by a grant from the Korean Ministry of Strategy and Finance under the Korea-World Bank Group Partnership Facility (KWPF) Trust Fund. The team gratefully acknowledges financial support from the Korean Ministry of Strategy and Finance that made this Project possible.

The Project team was headquartered in the World Bank, and included the following participating organizations: the Council of Europe (CoE), the International Association of Penal Law (AIDP), the International Telecommunication Union (ITU), the Korea Supreme Prosecutors Office (KSPO), the Oxford Cyber-security Capacity Building Centre (Oxford), the United Nations Conference on Trade & Development (UNCTAD), the United Nations Interregional Crime and Justice Research Institute (UNICRI) and the United Nations Office on Drugs & Crime (UNODC).

The Project team at the World Bank was led by David Satola and included Seunghyun Bahn, Evarist Baimu, Nigel Marc Bartlett, Jinyong Chung, Conrad C. Daly, Heike Gramckow, Theodore Christopher Kouts, Clay Lin, Rishabh Malhotra, James Neumann, Marco Nicoli, Diana Norman, Elizabeth Anne Norton, Seunghwan Park, Sandra Sargent, Dolie Schein, Hyunji Song, Emilio C. Viano, Georgina Weise, Christiaan van der Does de Willebois, Stuart Yikona, Keong Min Yoon and Tamika Zaun.

The Team owes a special debt of gratitude to Hyunji Song, for her unflagging commitment and contributions to this project too numerous to mention here. Without her research and organizational skills, initial drafting efforts and intellectual guidance, this Project could not have been realized.

The contributions of the following people from the participating organizations are recognized. From KSPO, Youngdae Kim, Seokjo Yang, Heesuk Lee and Seungjin Choi. Luc Dandurand, Marco Obiso, Preetam Maloor and Rosheen Awotar-Mauree of ITU; Francesca Bosco and Arthur Brocato of UNICRI; Sadie Creese, Eva Ignatuschtschenko and Lara Pace of Oxford; Cecile Barayre of UNCTAD; Alexander Seger and Betty Shave of CoE; and Neil Walsh, Dimosthenis Chrysikos and Bilal Sen of UNODC.

The Team would also like to express its gratitude to peer reviewers, Professor Ian Walden, Queen Mary University of London, and Steven Malby of the Commonwealth. The team is also grateful for the time, consultations and valuable inputs received from staff at INTERPOL's Global Complex for Innovation in Singapore including Madan Oberoi, Mustafa Erten, Steve Honiss, Silvino Schlickmann and Tomas Herko.

The Toolkit and Assessment Tool were also the subject of several consultation events, conferences and workshops held at or with the sponsorship of the CoE, Europol, INTERPOL, ITU, the Korea Institute of Criminology, UNCTAD, UN and Central Bank of Qatar. The team thanks the participants in all of these events and at these organizations for the opportunities to raise awareness of this Project and for helpful comments and suggestions.

The team apologizes to any individuals or organizations inadvertently omitted from this list.

The Toolkit, Assessment Tool, and Website designed and developed by Informatics Studio: www.informatics-studio.com.

Foreword

Advances in technologies over the last 20 years have affected virtually every aspect of the way we live and conduct our daily lives. While these technologies have been a source of good and enabled social and economic progress around the world, hardly a day goes by without news of yet another cyberattack, or the use of technology in the commission of crime. Here, at the World Bank, we know that in order for technologies, including the internet, to continue to be used as a force for economic growth and development, measures must be taken to ensure the security of the internet and the data and communications that flow over it.

This book, ***Combatting Cybercrime: Tools and Capacity Building for Emerging Economies,*** is an important contribution to the global effort for a safe, secure and equitable internet. It focuses on building the human capacity of policy-makers, legislators, judges, lawyers, prosecutors, investigators and civil society on the various legal issues that comprise the fight against cybercrime. Though focusing on legal matters, ***Combatting Cybercrime*** recognizes that the challenge is much larger, and, accordingly, builds from the perspective that an effective response to ever-more sophisticated cybercrime requires a multidisciplinary, multi-stakeholder, public-private approach.

In addition to serving as a resource in the traditional sense, ***Combatting Cybercrime*** includes an online Assessment Tool that enables countries to more accurately identify priority areas, that facilitates a focused and targeted allocation of scarce, capacity-building resources.

Much like the collective approach that is required to fight cybercrime, ***Combatting Cybercrime*** is also the result of a collective effort among some of the key global and regional organizations, both public and private, whose expertise and experience are synthesized in this book. I would like to thank the organizations and their staff who contributed to this important work, as well as the Government of Korea for its generous funding and leadership in this area that made ***Combatting Cybercrime*** possible.

It is our collective hope that ***Combatting Cybercrime*** will be a useful resource in building capacity on these key legal issues in the global fight against cybercrime, and would invite readers to consult the project website for updates. The Toolkit, the Assessment Tool and a library of pertinent sources can be found and freely accessed at www.combattingcybercrime.org.

Sandie Okoro
Senior Vice President and General Counsel
The World Bank

Table of Contents

Abbreviations & Acronyms

ACHPR	African Commission on Human and Peoples' Rights
ACHR	American Convention on Human Rights
AI	Artificial Intelligence
ALADI	Asociación Latinoamericana de Integración
AML	Anti-money Laundering
AP-CERT	Asia Pacific Computer Emergency Response Team
APEC	Asia-Pacific Economic Cooperation
ASEAN	Association of Southeast Asian Nations
ATM	Automated Teller Machine
BEC	Business Email Compromise
CCI	Commonwealth Cybercrime Initiative
CCIPS	Computer Crime and Intellectual Property Section
CCPCJ	Commission on Crime Prevention and Criminal Justice
CERT	Computer Emergency Response Team (or Computer Emergency Readiness Team)
CETS	Child Exploitation Tracking System
CFTT	Computer Forensics Tool Testing
CIRT	Computer Incidence Response Team
CIS	Commonwealth of Independent States
CJEU	Court of Justice of the European Union
COMESA	Common Market for Eastern and Southern Africa
CoE	Council of Europe
COMSEC	Commonwealth Secretariat
cPPP	Contractual Public-Private Partnership
C-PROC	CoE Cybercrime Programme Office
CSIRT	Computer Security Incident Response Team
CSIS	Center for Strategic and International Studies
CTO	Commonwealth Telecommunications Organisation
DC3	US Defense Cyber Crime Center
DDBMS	Distributed Database Management System
DDoS	Distributed Denial of Service
DEA	US Drug Enforcement Agency
DHS	US Department of Homeland Security
DNS	Domain Name System
DoD	US Department of Defense
DoJ	US Department of Justice
DoS	Denial of Service
E2EE	End-to-end Encryption
EAC	East African Community
EaP	EU Eastern Partnership
EC3	European Cybercrime Centre
ECHR	European Convention on Human Rights
ECJ	European Court of Justice
ECtHR	European Court of Human Rights
ECOWAS	Economic Community of West African States
ECTF	US Secret Service Electronic Crimes Task Force
EJN	European Judicial Network
ENISA	European Network and Information Security Agency
EU	European Union
EUISS	EU Institute for Security Studies
EUROJUST	EU Judicial Cooperation Unit
EUROPOL	European Police Office
FBI	US Federal Bureau of Investigation
FOI	Freedom of Information
G8	Group of Eight
GCA	ITU Global Cybersecurity Agenda
GCI	ITU Global Cybersecurity Index
GCSCC	Global Cyber Security Capacity Centre (Oxford University's Martin School)
GLACY	Global Action on Cybercrime (CoE & EU)
GLACY+	Global Action on Cybercrime Extended (CoE & EU)
GPEN	Global Prosecutors E-crime Network
GPS	Global Positioning System
HIPCAR	Harmonization of ICT Policies, Legislation and Regulatory Procedures in the Caribbean
HIPSSA	Harmonization of ICT Policies in Sub-saharan Africa
IADB	Inter-American Development Bank
IAP	International Association of Prosecutors
IAPL	International Association of Penal Law
IBRD	International Bank for Reconstruction and Development
IC3	Internet Crime Complaint Center
ICB4PAC	Information and Communications Capacity Building for Pacific Island Countries
ICCPR	International Covenant on Civil and Political Rights
ICT	Information and Communication Technology
IDCC	INTERPOL Digital Crime Centre

IoE	Internet of Everything
IGCI	INTERPOL Global Complex for Innovation
IGO	Intergovernmental Organization
INTERPOL	International Criminal Police Organization
IOSCO	International Organization of Securities Commissions
IoT	Internet of Things
IP	Internet Protocol
iPROCEEDS	Cooperation on Cybercrime under the Instrument of Pre-accession (IPA)
ISAC	Intelligence Sharing and Analysis Center
ISP	Internet Service Provider
IT	Information Technology
ITU	International Telecommunication Union
J-CAT	Joint Cybercrime Action Taskforce
JIT	Joint Investigation Team
JPIIT	KSPO's Joint Personal Information Investigation Team
KSPO	Korean Supreme Prosecutor's Office
MA	Mutual Assistance
MLA	Mutual Legal Assistance
MLAT	Mutual Legal Assistance Treaty
MSN	Microsoft Service Network
NCA	UK National Crime Agency
NCB	National Central Bureau
NCCIC	US National Cybersecurity and Communications Integration Center
NCFTA	National Cyber-Forensics & Training Alliance
NCIJTF	FBI's National Cyber Investigative Joint Task Force
NCRP	National Central Reference Points
NCS	National Cybercrime Strategy
NIST	US National Institute of Standards and Technology
NSA	US National Security Agency
OAS	Organization of American States
OCSI	UK Office of Cyber Security and Information
OECD	Organization for Economic Co-operation and Development
OECS	Organization of Eastern Caribbean States
OSCE	Organization for Security and Co-operation in Europe
OTP	One-time Pad
P2P	Peer-to-peer
PIN	Personal Identification Number
PPP	Public-Private Partnership
R&I	Research and Innovation
RTI	Right to information
RICO	US Racketeer Influenced Corrupt Practices Act
SADC	Southern African Development Community
SAR	Suspicious Activity Reporting
SCO	Shanghai Cooperation Organization
SDG	Sustainable Development Goa
SELA	*El Sistema Económico Latinoamericano y del Caribe*
SIM	Subscriber Identification Modulel
SME	Small & Medium Sized Enterprise
SMS	Short Message Service
SNS	Social Networking Service
SQL	Structured Query Language
SQLi	Structured Query Language Injection
SWIFT	Society for Worldwide Interbank Financial Telecommunication
T-CY	CoE Cybercrime Convention Committee
Tor	The Onion Router
UDHR	Universal Declaration of Human Rights
UK-CERT	UK Computer Emergency Response Team
UN	United Nations
UNAFEI	UN Asia and Far East Institute for the Prevention of Crime and the Treatment of Offenders
UNCITRAL	UN Commission on International Trade Law
UNCTAD	UN Conference on Trade and Development
UNESCO	UN Educational, Scientific and Cultural Organization
UNHRC	UN Human Rights Council
UNICRI	UN Interregional Crime and Justice Research Institute
UNODC	UN Office on Drugs and Crime
USB	Universal Serial Bus
US-CERT	US Computer Emergency Response Team
USSS	US Secret Service
VoIP	Voice-over Internet Protocol
VPN	Virtual Private Network
VR	Virtual Reality
WDR	World Bank *World Development Report: Digital Dividends* (2016)
WEF	World Economic Forum
WSIS	World Summit on Information Society

Introductory Part

This chapter sets the stage for the rest of the Toolkit. It provides an overall introduction to the Toolkit, highlights some of the main the issues around cybercrime and describes some of the main challenges to fighting cybercrime.

In this Chapter

A. Purpose of Toolkit

Table of Contents

I. Background

Hardly a day goes by without the press disclosing some major cyber-incident. The past year alone has witnessed a proliferation of cyberthreats, breaches of corporate and governmental networks, major thefts from banks, malware, ransomware, etc. Here are a few notable incidents:

- McAfee reports 316 threats every second[1]
- Theft of US$81 million from account of Bangladesh at New York Federal Reserve Bank resulting from alleged compromise of SWIFT network[2]
- 1 billion hacked Yahoo! accounts[3]

But cybercrime is not limited to major breaches. Individuals also suffer from threats, exploitation and harassment, or worse. The internet, which has enriched peoples' lives and made the world a "smaller" place, also enables a range of criminal activity.

One recent study[4] finds that, while cyberthreats mainly consisted of viruses, worms and Trojans, over time cybercriminals have begun to take advantage of techniques related to social engineering—such as phishing—that target employees having direct access to databases containing confidential business information, as well as pharming, credit card fraud, dedicated denial-of-service (DDoS) attacks, identity theft and data theft. According to a Special Eurobarometer commissioned by the European Union (EU), the majority of internet users across the EU do not feel that making online purchases or doing online banking is secure, and have no idea how to navigate the internet safely.[5] Many respondents claim to know about cybercrime from newspapers or television, but do not feel informed about the risks that may be experienced. Cybercriminals exploit this lack of awareness.

The same study found that more than a third of internet users claim to have received at least one email scam and feel concerned about their sensitive data online.[6] Considering the increasing number of people in possession of at least one smart device, and the increasing use of such

devices as business tools, it is easy to see that there is plenty of fertile ground in which cybercrime can operate and grow.

As cyberspace is rapidly evolving, the cyberthreats of the recent past also have also changed. They have not only multiplied with respect to the means through which they are perpetrated, but also have evolved into cybercrime, cyberterrorism, cyberespionage, cyberwarfare and hacktivism.[7] The universe of cybercrime is huge and includes different types of attacks and attackers, risks and threats.

The challenge, therefore, is how to combat such diverse criminal activity and yet to preserve the many positive aspects of our interconnected world.

II. The Toolkit

This Toolkit, *Combating Cybercrime: Tools and Capacity Building for Emerging Economies,* aims at building capacity to combat cybercrime among policy-makers, legislators, public prosecutors and investigators, as well as among individuals and in civil society at large in developing countries by providing a synthesis of good practices in the policy, legal and criminal-justice aspects of the enabling environment necessary to combat cybercrime. Included in this Toolkit is an Assessment Tool that enables countries to assess their current capacity to combat cybercrime and identify capacity-building priorities (discussed in more detail in chapter 7, and included in appendix 9 E). The Toolkit is also accompanied by a Virtual Library, with materials provided by participating organizations and others.[8]

There are no shortages of resources regarding combatting cybercrime. An overriding ethos of the organizations (listed below) participating in the development of this Toolkit was to avoid repeating or replicating existing resources. However, it was felt that there was merit to producing a synthetic reference on combatting cybercrime, taking best practices and packaging them in a new, holistic fashion. In that sense, the Toolkit can be viewed as a kind of "portal", overview or one-stop shop that directs users who want to learn more or to go deeper into a particular topic, as well as developing a framework to better understand how seemingly disparate issues interrelate and providing some direction on how to get to primary resources.

The Toolkit is arranged along the following lines. In the introductory chapter, the Toolkit examines the current landscape of cybercrime and some of the challenges are to combatting cybercrime. In chapter 2, the Toolkit then looks at some foundational issues including what is meant by and what constitutes cybercrime, and then looks at procedural, evidentiary, jurisdictional and institutional issues. The Toolkit goes on to consider formal and informal measures of international cooperation in chapter 3. In chapter 4, the Toolkit explores national legal frameworks. Chapter 5 examines in detail at due process, data protection and freedom of expression safeguards. Chapter 6 looks at different aspects of capacity-building. Chapter 7 explores various assessment tools, including

the Assessment Tool developed under this Project. Some concluding observations can be found in chapter 8. The Toolkit also contains appendices regarding cybercrime cases, multilateral instruments, national legal frameworks and the various assessment tools.

III. The Assessment Tool

The Toolkit, a reference resource on its own, provides a broad contextual background to the Assessment Tool. The Toolkit and Assessment Tool should be read together.

The Assessment Tool follows the same general organization as the Toolkit and assesses capacity readiness using some 115 indicators and is organized along the following nine dimensions:

1. Policy Framework
2. Legal Framework
3. Substantive Criminal Law
4. Procedural Criminal Law
5. e-Evidence
6. Jurisdiction
7. Safeguards
8. International Cooperation
9. Capacity-building

IV. The Broader Context

While this Toolkit and the Assessment Tool look at capacity building to combat cybercrime primarily from a legal perspective, it is recognized that combatting cybercrime is a part of a broader effort to ensure cybersecurity. Accordingly, this Toolkit puts cybercrime in a broader cybersecurity context. And while it is primarily legal, it also looks at the role of the private sector and technical community, including CIRTs and the like,[9] in combatting cybercrime. But because the Toolkit mainly approaches combatting cybercrime from a legal perspective, every effort has been made to illustrate the various aspects of cybercrime through the use of court cases. Almost by definition, if a case ends up in the courts, it is because there is a disputed issue of law. These cases are referred to and highlighted as "cases" in the text of the Toolkit. These cases are used throughout the Toolkit but are also aggregated in appendix 9 A. Of course, not all issues, even if they involve criminal activity, end up in the courts. Accordingly, not every aspect of combatting cybercrime is supported by a case. However, the Toolkit also uses case studies to illustrate some aspects of combatting cybercrime. These are referred to and included in "boxes" throughout the Toolkit. In its synthetic approach, the Toolkit also attempts to include different legal systems.

As discussed above, and explored in more depth in sections 2 A and 2 B, the Toolkit has attempted to include not only more "traditional" cybercrimes, but also "new" kinds of crime committed on or

using the internet. Importantly, and for the reasons described herein, the Toolkit adopts a definition of "cybercrime" (*see* section 2 A, below) for the purposes of this Toolkit that attempts to be "future proof"—that is, a definition that is broad enough to encompass already well-known types of crimes, but also new and evolving areas, such as risk posed by cloud and quantum computing, blockchain technologies and digital currencies, the internet of things (IoT), etc.

The Toolkit also places emphasis on the safeguards accompanying cybersecurity (considerations of "due process" and ensuring freedom of expression and privacy/data protection). As a general proposition, the "balance" to be achieved between security and preservation of basic rights was recently given prominence of place in the World Bank's ***World Development Report 2016: Digital Dividends*** (WDR).[10]

At the same time, the Toolkit is about cybercrime and not cyberterrorism or cyberwar. Admittedly, it is becoming increasingly difficult to distinguish between acts that might first appear to be "mere" cybercrime perpetrated by civilian actors, but that may emerge with the passage of time and further investigation to be acts by states against states (or their proxies).[11] Indeed, cyberspace has been recognized as a sovereign domain, akin to air, land and sea.[12] That relationship and blurring of lines between cybercrime and cyberwar is beyond the scope of this work and will have to be the subject of another work.

It is axiomatic to say that cybercrime is continually evolving. Accordingly, the Toolkit captures information as of 1 January 2017 and will be periodically updated.

It should also go without saying that nothing in this Toolkit constitutes legal advice and no inference should be drawn as to the completeness, adequacy, accuracy or suitability of any of the analyses or recommendations in it to any particular circumstance. All information contained in the Toolkit may be updated, modified or amended at any time.

V. Participating Organizations

- *Association Internationale de Droit Pénal*
- Council of Europe (CoE)
- International Telecommunication Union (ITU)
- Supreme Prosecutors' Office of Republic of Korea (KSPO)
- Global Cyber Security Capacity Building Centre located at the Martin School at Oxford University (Oxford)
- United Nations Conference on Trade and Development (UNCTAD)
- United Nations Interregional Crime and Justice Research Institute (UNICRI)
- United Nations Office on Drugs and Crime (UNODC)

This work has been funded by the Government of Korea through a grant provided by the Korea-World Bank Group Partnership Facility.

B. Phenomenon & Dimensions of Cybercrime[1]

Table of Contents

Introduction

Having set forth the purpose of the Toolkit in section 1 A, we now look at some of the particular features of cybercrime in its evolving context. This section begins by **(I)** talking about the place of cyberspace in today's world and the place of the law therein, going on to **(II)** drawing attention to the important role of private sector engagement.

I. Situating Cyberspace

Law, as a reflection of public policy, is intended to provide a predictable, fair and transparent basis for ordering society, and for offering objective means for dispute resolution. With **(A)** the society's expansion into "cyberspace"[2] ushering in a brave new world, it is fundamental that **(B)** public confidence in law and order also extends into cyberspace in order for that space to continue to be a place where economic, political and social discourse flourish. But because **(C)** cybercrime is not entirely virtual or physical, **(D)** innovative public policy and legal approaches addressing cybercrime—balancing security with human right—are imperative.

A. "A Brave New World"[3]

Cyberspace is a nebulous digital or electronic realm characterized by the use of electronics and electromagnetics to store, modify and exchange data via networked systems and associated physical infrastructures. Not a "place" *per se*, it has been defined as "the online world of computer networks",[4] but has been more aptly likened to the "human psyche translated to the internet".[5]

However it is understood, cyberspace has transformed the world and our way of being. It has created a "virtual" space parallel to the "real", physical world. And, although not actually real, that revolutionary world is itself about to be revolutionized as virtual reality (VR) prepares to render further transformations, no doubt with great implications for the "real" world,[6] and, indeed, for what "real" means.[7] Information and communications technologies (ICTs) allow for information to be accessed, business conducted, professional and personal connections grown and maintained, and governments engaged and governance expanded. Cyberspace and ICTs hold out huge growth potential in practically every walk of life.[8]

With this greater openness, interconnectedness and dependency also comes greater risk: while ICT has created new and legitimate opportunities, spaces and markets, those very same opportunities, spaces and markets are rife for criminal exploitation. Individual cybercriminals and organized criminal groups are increasingly using digital technologies to facilitate their illegal activities, be they the enabling of traditional crimes, such as theft and fraud, or the rendering of new crimes, such as attacks on computer hardware and software. Even in countries characterized by high rates of unemployment, wage inequality and poverty, cybercrime is accessible, easy and cheap. Essentially, anyone with access to the internet can become a cybercriminal. Moreover, with the emergence of hacking tools, such as exploit-kits, neither computer expertise nor technological knowledge is longer necessary.[9] People in developing countries, often unable to find legitimate work in their domestic market, see cyberspace, with more than 3.488 billion internet users worldwide,[10] as a market ripe for exploitation.[11] Governments are coming to recognize both the harm that has been caused, as well as the ever-growing gravity of the threat cybercrime, and are working on forming a collaborative response at both the domestic and international levels.

That collaborative, international response to cybercrime cannot come soon enough: cybercrime is on the rise, and the opportunities and gains are increasingly alluring.

In 2014, more than 348 million identities were exposed

When identity thieves hacked several trusted institutions, and 594 million persons are affected by cybercrime globally.[12]

US$1 trillion in the United States

Estimates of losses from intellectual property and data theft go as high as US$1 trillion in the United States alone.[13]

170 million credit and debit card numbers stolen

In 2010, a hacker was sentenced to twenty years in prison for stealing more than 170 million credit and debit card numbers, making it the largest single-identity theft case that the US Department of Justice (DoJ) has ever prosecuted.[14]

Case 1.1: FBI Hacks "Playpen" Child Pornography Site on Tor Network (USA)[15]

In a massive sting operation, FBI agents infiltrated "Playpen", one of the largest ever child pornography networks, by infecting websites with malware that bypassed user's security systems.[16] The FBI continued to operate the site for thirteen days after it had secured control of it, subsequently identifying hundreds of users.

Tor—an abbreviation for "The Onion Router"—is a free software that allows anonymous internet communication, preventing localization of users or monitoring of browsing habits, by bouncing users' internet traffic from one computer to another to make it largely untraceable.[17] Operating through the special-use, top level domain suffix ".onion",[18] Tor addresses are not actual names in the domain name system (DNS)—the hierarchical, decentralized naming system for computers, services or any resource connected to the internet or a private network. Initially developed with the US Navy, today it is a nonprofit organization; the, Tor network is a group of volunteer-operated servers.

Tor's popularity recently increased with its launch of a hidden chat tool that not only hides message contents from everyone except participants, as well as hiding the location of those participants, but which also operates with platforms such as Facebook Chat, Google Talk, Twitter and Yahoo!, even in countries where those platforms are banned.[19] Rather than rely on the "dark web", a collection of hidden websites and services of which Tor forms a prominent part, the Tor Messenger operates by sending messages across a series of internet relays (or routers), known as "bridges", thereby masking the messages' origins.[20] Because the services operate through a collection of relays that are not publicly listed, blocking access to the Tor network would not affect the Tor Messenger.[21] Furthermore, just as with services such as WhatsApp (*see* section 1 B, case 1.3, below), end-to-end message encryption may be offered. Although concern exists that the services might be used for more nefarious purposes, there is public interest in having such a tool—for instance, for whistleblowers and others needing anonymity. While banning Tor might well be both infeasible and unwise,[22] this case indicates that Tor is not a perfect blanket of anonymity.

B. Maintaining Public Confidence

One of the principal purposes of the law is to provide an objective, predictable, transparent and universally-applicable set of rules that governs conduct and maintains order.[23] A key element to order is public confidence,[24] which is bolstered through laws supported by principles of transparency, accountability and participation. It is well understood that "trust" in the use of the internet and ICTs will engender use, and that part of building this trust environment in cyberspace involves striking a balance between establishing the security of networks, devices and data, and ensuring that fundamental rights such as privacy (including data protection) and freedom of expression are observed.[25] The evolution of cyberspace, and the ever-increasingly easy means of accessing it, have resulted in a new range of living and coexisting, which society—and the law—are grappling to understand.[26] These new, exciting possibilities should not be either unnecessarily or disproportionately stifled in the name of security and combating criminality.

Nature abhorring a vacuum,[27] and the path of least resistance being preferred,[28] society at large—individuals, financial institutions, private industry and governments—have increasingly exploited, and subsequently come to rely on technology in order to function: cyber networks have become essential to everyday operations, with power grids, air traffic control, urban utilities and much more dependent upon cyber technology.[29] Consequentially, the potential threat posed by cybercriminals has grown dramatically and afforded significant opportunities for terrorist groups and extremist organizations.

Public confidence in the secure functioning of ICT systems and of cyberspace has become necessary to maintaining social order.[30] Several legal systems stress the need to protect the functioning of ICT systems through criminal laws.[31] The principal protected interests are the confidentiality, integrity and availability of information systems and electronic data.[32] In pursuit of the urgency to criminalize certain behavior, the challenge in terms of law reform is to avoid overreaching in order not to violate fundamental rights.[33]

C. Cybercrime's Physical & Virtual Nature

While this Toolkit expands in more detail in subsequent chapters both the working definition of cybercrime (*see* section 2 A, below) as well as what sort of acts constitute cybercrime (*see* section 2 B, below), in many cases, cybercrime can be understood as digital versions of well-known, "traditional" offenses only with a virtual or cyberspatial dimension in addition or *in lieu* of.[34]

For instance, identity theft, which can happen in both the physical and electronic worlds, fits an adaptive conception of cybercrime perfectly well. The factor differentiating identity theft in the physical and virtual worlds is the crime's "how". In both instances, the criminal intent (namely, to obtain a benefit) and the result (namely, fraudulent misrepresentation) are the same.[35] The "how" differs in that, in the physical version, the impersonation is done with a physical item (*e.g.,* a stolen identity card, mail, statement), while, in the virtual version, the crime is committed through the

presentation, usually to some remote, automated interface, of identifying information (*e.g.*, a password). In the virtual setting, the cybercriminal may fraudulently induce someone to voluntarily reveal that information or use automated "keystroke logging" software to record an electronic copy of that information and relay it to the cybercriminal.

While the two paradigms are relatively comparable, transitional difficulties arise at the level of law enforcement.[36] For instance, police, frequently accustomed to building a physical record—a physical "paper trail"—, often have difficulty transposing that record to the electronic world and investigating on purely electronic grounds.[37]

Problems in conceptualization are often complicated or reinforced by laws that remain outpaced by technological developments.[38] As a result, law enforcement often lags far behind the pioneers of organized crime.[39] For example, in the United States, computer fraud (criminalized in 18 USC § 1030) is not yet classified as a predicate offense for racketeering under the Racketeer Influenced Corrupt Practices (RICO) Act.[40] One of the most important tools to combat organized crime,[41] RICO, which allows for leaders of crime syndicates to be targeted, came to prominence in the 1980ˢ when its provisions began to be applied to combat the mafia.[42]

Cyberspace has allowed criminals to more "efficiently" commit crimes.[43] Electronic tools and equipment, many of which are freely available on the internet, can be ordered and distributed with just one mouse-click, yet frequently affecting millions. Examples of "computerized" or "electronic" versions of traditional crimes include ICT-mediated fraud, revelation of electronically-stored secrets, forging digitally-stored data, defamation, cyberstalking, copyright violation and cyber-bullying.[44] In such instances, the affected interests remain the same, with only the *modus operandi* differing from the traditional form.[45]

In many cases, cyberspace has made committing crimes so much simpler that the use of the electronic medium has eclipsed using traditional ones. For instance, today, pornography (including child pornography) is principally transmitted and distributed electronically. Indeed, such behavior has even led some legal systems to introduce special criminal prohibitions against cyber pornography, with nuanced aspects unique to cyberspace being addressed—for instance, "grooming" of children for potential sexual abuse through electronic communications has also been defined as a criminal offense in many jurisdictions.[46] Where perpetrators use virtual social networks to initiate and establish physical contact in order to commit sexual offenses, they cross the line between the "traditional" crime type and the type of crime that depends on the existence of the internet.

Case 1.2: State of Tamil Nadu vs. Suhas Katti (India)[47]

Complainant, a divorced woman, was the subject of obscene, defamatory and harassing messages that were both posted online and which were sent to her from an email account falsely opened in Complainant's name. Defendant's postings, which released her phone

number without her consent, resulted in telephone calls to Complainant in the belief that she was soliciting sexual favors. Defendant, a purported family friend of Complainant, was apparently motivated by a desire to marry Complainant. When Complainant's marriage ended in divorce, Defendant resumed contact with her and, on her refusal to marry him, began his cyber harassment.

The court, relying on testimony from witnesses at the cyber café where the behavior took place, on experts, and on cyber forensic evidence, convicted Defendant of "transmitting obscene material in electronic form" under Section 67 of Information Technology Act 2000 (§§ 469 & 509, Indian Penal Code). The Act has drawn subsequent controversy as a vaguely worded criminal statute, predicated on the meaning of "obscene" material as one that could be used to curtail any sexually explicit material. While cybercrime has a fairly low conviction rate, this case, the first of its kind, was prosecuted in just seven months.

The first case of successful cybercrime conviction in India, and with such rapid conviction, this case represents a significant landmark in the fight against cybercrime.

D. Innovative Criminal Prohibitions

The relationship between virtual and physical worlds has meant that laws ordained for the physical world and to tangible property have sometimes been applied to cyberspace and to virtual property.[48] Applying physical-crime laws to cybercrime has been particularly prevalent with respect to theft and fraud, although doing so has met with varying degrees of success. On the one hand, in 2012, the Dutch Supreme Court confirmed a conviction for theft of electronic goods on the basis of existing, unadapted law.[49] Similarly, in the United States illegally acquiring or using another's "means of identification" with the intent to commit an unlawful act is a crime.[50] Elsewhere, computer forgery, fraud by false representation, wrongful impersonation of another person, defamation and dissemination of information violating another's personal privacy have all been accepted as crimes committed in cyberspace on the basis of physical-world crimes.[51] On the other hand, however, other legal systems have not always considered hacking as theft, typically on the basis that hacking normally does not "permanently deprive" the victim of the goods, and, as such, should be understood as a form of involuntary sharing, rather than theft.

Regardless of the answer to whether laws written for the physical world should be applied to the electronic world, legal systems have created corresponding categories and definitions of offenses[52] aimed specifically at protecting the substantial, new interests and opportunities possible in the cyberworld.[53] For example, a virtual version of harassment exists in many legal systems: cyberharassment has been defined as a person's "use [of] a network or electronic communications service or other electronic means to annoy or cause damage to his correspondent, or to install any device intended to commit the offense and the attempt to commit it".[54] Similarly, because the internet allows for the immediate dissemination of sensitive information and images in the absence

of consent,[55] cases of "revenge porn" (where material containing nudity or of sex activities is posted in revenge by erstwhile lovers in order to embarrass, punish or interfere with other relationships of the victim), are increasingly frequent and have received particular legal attention.[56]

Moreover, although the electronic and physical worlds are distinct from each other, the two are very much interconnected. For instance, regarding property, "cyber goods" have value and their loss can cause just as much harm as the loss of tangible property.[57] Moreover, stealing a person's virtual identity can have very serious repercussions in the physical world, and such identity theft is often a precursor to defrauding the victim in concrete, commercial transactions involving tangible goods.[58] For example, a perpetrator may illegally acquire the victim's access data, gain access to his bank account or, more simply, order and acquire goods, leaving the bill to the victim.[59] Still more troubling, the usurpation of a person's virtual identity can have serious and even irreparable consequences in both professional and personal circles; loss of reputation can be much more damaging than financial loss of online purchases.[60] Given the potentially great value of both reputation and integrity of cyber personalities and avatars, the usurpation or falsification of a person's virtual identity has been criminalized,[61] often regardless of whether there is intent to cause material harm.[62]

E. Technological Innovations

Recent technological developments have drawn increased attention on the importance of addressing how the physical and electronic worlds are to interrelate, and how to define the overall landscape of cyberspace. Although discussed in greater depth further on (*see* sections 1 C and 2 A, below).The most notable of these matters merit mentioning here:

These technological advances include developments in FinTech, horizontal data partitioning ("sharding"), blockchain, quantum computing and artificial intelligence:

- Reliance on ***FinTech*** or financial technology, will continue to grow as the technology-enabled financial solutions facilitated "smart" transactions and help removing transaction costs.[63] However, as FinTech continues to permeate everyday activities, it necessarily results in the collecting and agglomerating of sensitive information —notably unique metadata—, inevitably becoming a target for cybercriminals.[64]

- Various techniques are being developed to improve data and systems security. Key among them is the use of the ***horizontal data partitioning,*** a technique known as "sharding", whereby electronic data is stored and spread across multiple databases. Doing so means that unauthorized users will only be able to access a small portion of the data, which may not even be readable on its own, or will have to independently infiltrate several or all of the systems in order to have the full data set. For instance, this technique might separate out credit card numbers, or parts of those numbers, from the corresponding verification numbers.[65]

- ***Blockchain technology*** is anticipated to change how transactions are done. Blockchain is a distributed, open-source, peer-to-peer, public ledger that records ownership and value. It

removes the need for a third-party verification organization, as transactions recorded on a public ledger and are verified through consensus. It is inexpensive, easy to use and secure; presently, it is the most secure transaction method available.[66] Although the technology is perhaps best known for its use in digital currencies,[67] its potential utility is endless. Beyond finance, blockchain has the potential to revolutionize all exchanges of information—smart contracts, patent registration, voting, distribution of social benefits, records, etc.[68]

- More dramatic changes are promised by ***quantum computing.*** Quantum computing would, in essence, take the present, binary operating form to a multidimensional level (*see* section 1 C, box 1.2, below), thereby threatening to undermine existing encryption systems and their algorithms.[69] Faced with this challenge, new cryptology schemes are looking to quantum mechanics that would use photons, and rely on physics as a means of security.[70]
- Lastly, the role of ***artificial intelligence*** (AI) is a growing prospect. Modern technology such as machine learning and autonomous systems would allow computers to learn, reason and make decisions with minimal human involvement. For example, AI can detect a security breach immediately, whereas, in the past, it would take months. Correspondingly, AI might be used to commit cybercrime, therein presenting unique legal questions (*see* section 1 C, below).

II. Private Sector Cooperation

Governments have an obligation to assure public safety and security in the analog world.[71] The ease and speed of information-sharing between cybercriminals, and the disparateness of criminal activity, makes it difficult for law enforcement to keep up. However, much of the infrastructure undergirding cyberspace, and many of the means of communications operating in cyberspace, are controlled by nonstate actors. Such being the case, government efforts to combat cybercrime will have to rely on private sector involvement, notably through the use of public-private partnerships (PPPs).[72]

In order to combat cybercrime, not only are tailor-made tools complementing traditional approaches needed, but so, too, is a unified approach for building collaborative partnerships between law enforcement and the private sector. Gathering and analyzing digital data are key to investigating and prosecuting cybercrime cases. At both the international and national level, entities such as INTERPOL and the KSPO are coordinating with the private sector in the area of digital forensics. These issues are explored in more depth further on (*see* section 6 C, below).

To a large extent, content carriers, notably internet service providers (ISPs), are not subject to prosecution, even though criminal content or criminal activity may be carried out using their services, and even though ISPs often have unique access to essential data regarding criminal content or activity. ISPs also store customer-use data. Moreover, most ISPs are usually private entities. In order to encourage investment in provision of internet services and access to the internet, most jurisdictions afford some limited liability for ISPs on the basis of being "mere conduits" or intermediaries. Once coupled with privacy guarantees,[73] the basic and widespread position is that ISPs are unaware of the criminal activity in much the same way that a landlord or a telephone company might be unaware of the natures of activities occurring on the rented premises,

or carried across their telephone lines. By contrast, those arguing for ISPs to assume greater liability from the start prefer to construe ISPs as newspaper publishers who should be responsible for the material on their servers. That said, liability often attaches once ISPs become aware of illicit activity and fail to act accordingly. Similar liability attaches to other service providers, such as bulletin board operators and proprietary information providers. It has been argued that, while many have called for harmonization, "uniformity is both illusory and unnecessary".[74]

Cooperation with the private sector, including PPPs play a vital part in the fight against cybercrime, especially, and to reiterate, as the private sector, and not government, either owns or operates so much essential infrastructure and provides essential services. According to INTERPOL,

> "The complex and ever-changing nature of the cyber threat landscape requires high-level technical expertise, and it is essential that law enforcement collaborates across sectors to effectively combat cybercrime and enhance digital security."[75]

In announcing its support for PPP cybersecurity initiatives last year, the US White House observed that "[c]urrent [PPPs] in this space have at best unclear or ill-defined roles and responsibilities for the industry and government partners."[76] The vastness of cybercrime is beyond the means of government: law enforcement is both unprepared and unable to fully scale-up to a fast-growing threat landscape. The greater the communication and coordination between public and private sectors, the greater society's resilience and ability to evolve to meet cybersecurity threats.

However, there is a lack of cooperation between governments and the private sector on matters of cybersecurity. US President Barack Obama highlighted this concern with his Executive Order aiming at encouraging better information sharing between the public and private sectors on cyberattacks.[77] President Obama said the following:

> "[T]he cyber threat is one of the most serious challenges to national and economic security that we face as a nation" and that "the economic prosperity of the United States in the twenty-first century will depend on cyber security".[78]

In Europe,[79] only a handful of European countries have an established framework for PPPs on cybersecurity.[80]

Case 1.3: In the matter of the Search of an Apple iPhone (USA)[81]

Though not technically a "cybercrime" case, the FBI went to court to compel Apple, Inc. to create a software tool that would help the FBI gain access to a locked iPhone that belonged

to an alleged terrorist shooter in San Bernardino, California.[82] The suit was eventually dropped after an unidentified third party successfully cracked the 5C iPhone running iOS 9 software, at a cost of US$1.3 million to the FBI.[83]

This situation demonstrates the diversity of efforts required for combatting cybercrime, and is anecdotal of the technical limitations on a government's ability to access data to investigate and prosecute acts of terrorism or cybercrime without the input of the private sector. The case raised the debate over whether private technology companies' encryption technologies protect privacy or endanger the public by preventing law enforcement access to critical information. As cyberspace continues to evolve, innovated investigative tools will also correspondingly be required to enable effective law enforcement investigations. While this particular standoff has come to an end, the tension between a government's desire to access technology and data necessary to enable effective investigation and the private sector's legitimate interest in providing secure technology and services to consumers as well as protecting proprietary investments has not. Moreover, while this suit was dropped, the US Government has since initiated other proceedings to compel Apple to assist the FBI in unlocking an iPhone 5s running iOS 7, though this time involving a "routine drug case".[84]

This incident also demonstrates that perfectly legitimate products—in this case, an iPhone—have become central to committing cybercrimes. Such technology, although only incidentally being used to support criminal activity, is being developed by a multitude of private actors. The government's ability to cover the great diversity of fields and spaces is well-beyond present budgetary constraints, illustrating the necessity of public-private cooperation. The public-private problem is only likely to grow, as not only Apple[85] but other technology firms, such as WhatsApp,[86] extend security and protection with end-to-end encryption (E2EE) and other security measures.

Indeed, following the 2017 terrorist attack outside the UK Houses of Parliament in London in March, and again following those in Manchester in June, UK authorities recently advocated that similar access should be granted vis-à-vis instant-messaging services, most notably for WhatsApp.[87] While the UK Home Secretary has sought to enlist the support of technology and social media at large,[88] the UK Prime Minister having repeated as much,[89] it seems unlikely that, even with private-sector cooperation, the problem would ever be resolved: simply put, the technological ease of encrypting communications means that a rival app or process is likely to appear almost immediately should present instant messaging systems be obliged to create such a "back door" for government. Moreover, lowered technological barriers to entry are bolstered by market demand, which, for numerous reasons—many of which are legitimate and legal—incentivizes the development of secure, anonymous communication tools.

Creating a strong legal cybersecurity framework is complex. The fundamentals of doing so range from establishing strong legal foundations and a comprehensive and regularly updated cybersecurity strategy, to engendering trust, working in partnership and promoting cybersecurity

education. These building blocks provide valuable guidance for governments that are ultimately responsible for implementing cybersecurity rules and policies.[90]

Conclusion

Although all of the following matters are addressed in greater depth in the Toolkit, a few points bear mentioning given this section's discussion:

- ***Cyberworld is a burgeoning space:*** In 2016, over 3.488 billion people, roughly forty percent of the world's population, used the internet.[91] Over sixty percent of all internet users are in developing countries, with forty-five percent of all internet users below the age of twenty-five years. By the end of the year 2017, it is estimated that mobile broadband subscriptions will approach seventy percent of the world's total population. By 2020, the number of networked devices (the "internet of things" (IoT)) will outnumber people by six to one, completely transforming current conceptions of the internet; moreover, interconnectivity will not be limited to the networking of devices but will also extend to humans, both at the individual and collective level (the "internet of everything" (IoE)).[92] In the hyper-connected world of tomorrow, it will become hard to imagine a "computer crime", and perhaps any crime, that does not involve electronic evidence linked with internet protocol (IP) connectivity. The greatest growth in the internet in the coming years will be the developing world because that is where the world's next billion people will access the internet for the first time.[93] It follows from that that the developing world is also where the greatest need will be to put in place policy and legal approaches for dealing with cybersecurity and cybercrime.

- ***Defining cybercrime poses difficulties*** (*see* section 2 A, below): A limited number of acts against the confidentiality, integrity and availability of computer data or systems represent the core of cybercrime. Beyond this, however, computer-related acts for personal or financial gain or harm, including forms of identity-related crime, and computer content-related acts (all of which fall within a wider meaning of the term "cybercrime") do not lend themselves easily to efforts to arrive at legal definitions of the aggregate term. Certain definitions are required for the core of cybercrime acts. However, a "definition" of cybercrime is not as relevant for other purposes, such as defining the scope of specialized investigative and international cooperation powers, which are better focused on electronic evidence for any crime, rather than a broad, artificial "cybercrime" construct.

- ***Cybercrime is global and occurs across sectors:*** Globally, cybercrime is broadly distributed across financially-driven acts, computer-content related acts, and acts against the confidentiality, integrity, and accessibility of computer systems. Perceptions of relative risk and threat vary, however, between governments and private sector enterprises. Currently, crime statistics may not represent a sound basis for cross-national comparisons, although such statistics are often important for policy making at the national level.

- ***International legal instruments have done much to spread increase knowledge sharing*** (*see* section 3 A, below): Legal measures play a key role in the prevention and combatting of cybercrime. These are required in all areas, including criminalization, procedural powers,

jurisdiction, international cooperation and ISP responsibility and liability. The last decade has seen significant developments in the promulgation of international and regional instruments aimed at countering cybercrime. These include binding and non-binding instruments. Five clusters can be identified, consisting of instruments developed in the context of, or inspired by: (1) the Council of Europe or the European Union, (2) the Commonwealth of Independent States or the Shanghai Cooperation Organization, (3) intergovernmental African organizations, (4) the League of Arab States, and (5) the United Nations. A significant amount of cross-fertilization exists between all instruments, including, in particular, concepts and approaches developed in the Council of Europe Convention on Cybercrime (the "Budapest Convention").

- ***There is a risk of partition between cooperating with shared cybercrime procedures and non-cooperating states*** (*see* section 3 A, below): Current international cooperation risks fall into two country clusters: those states that have implemented reciprocal powers and procedures to cooperate among themselves, and those that have failed to implement those measures, are restricted to "traditional" modes of international cooperation that take no account of the specificities of electronic evidence and the global nature of cybercrime. Such a concern is particularly true of investigative actions. The lack of a common approach, including within current multilateral cybercrime instruments, means that even simple requests for actions, such data preservation, may not be easily fulfilled.

- ***Regulatory frameworks must maintain data integrity while protecting freedoms:*** Regulatory frameworks, essential to the fight cybercrime, must be sufficiently bolstered to assure freedom of speech and access to information. Relatedly, while data protection laws generally require personal data to be deleted when no longer required, some states have made exceptions for purposes of criminal investigation, requiring ISPs to store specific types of data for a set period of time. Many developed countries also have rules requiring organizations to notify individuals and regulators of data breaches. Also, while it might be technically possible for ISPs to filter content, any restrictions that they place on internet access are subject to both foreseeability and proportionality requirements under international human rights law protecting rights to seek, receive and impart information.

- ***The question of holding ISPs liable:*** Following directly on from the previous matter is the question of whether, and to what extent, to hold ISPs liable for objectionable content is a vast one. In many legal systems, ISPs may be held liable for failing to control or constrain illegal content or activity crossing their systems. In other systems, however, that liability is limited on the basis that ISPs are "mere conduits" of data. That said, where liability is limited, it can often shift to a requirement to take action if an element of content-awareness becomes apparent—for instance, where the ISP modifies transmitted content or if actual or constructive knowledge of illegal activity or content is shown.

- ***PPPs are central to cybercrime prevention:*** PPPs are created as much by informal agreement as by legal basis. Private sector entities tend to be most frequently involved in partnerships, followed by academic institutions, and then by international and regional organizations. PPPs are mostly used to facilitate knowledge sharing, though they have been used, especially by private-sector entities, to prompt investigation and legal actions. Such actions complement those of law enforcement and can help mitigate damage to victims. Academic institutions play a variety of roles in preventing cybercrime, including training, developing law and policy development, and technical standards setting, as well as housing cybercrime experts, computer emergency response teams CIRTs and specialized research centers.

C. Challenges to Fighting Cybercrime

Table of Contents

Introduction

Recent ICT developments have not only allowed for the emergence of new types of illegal activities, but have also resulted in novel techniques for evading law enforcement authorities, and, even after having been found out, in hindering investigation and prosecution. At the same time, ICT advancements have strengthened the abilities of law enforcement agencies to investigate and prosecute cybercriminals.[1] This section examines challenges in the fight against cybercrime.

This section begins by **(I)** talking of general challenges to cybercrime, goes on to **(II)** talk about specific challenges of developing legal frameworks, and then **(III)** highlights that there are other resources that might be brought to bear. The last half of the section

discusses **(IV)** the various challenges of a lack of international interoperability and **(V)** the need for appropriate safeguards to be implemented by both national and international authorities.

I. General Challenges

Challenges to investigating and prosecuting cybercrime arise out of its transnational, and thus multi-jurisdictional, nature, as well as to challenges in detecting these crimes, insufficient legal frameworks and the ever-shifting technological landscape.

Technology moves on apace, and usually much more quickly than authorities or, even more so, legislatures do. Bearing such technological evolution in mind, legislatures frequently attempt to account for technological progress that would render the wording of a criminal statute obsolete by, for instance, using relatively generic language and not specifying technology, or by adopting generalizations—for instance, "any electronic communication technology, regardless of its technological format or appearance".[2]

Challenges for law enforcement in the fight against cybercrime are manifold. The most common include the following:

1. Growing access to high-speed internet access;
2. Growing availability of hardware and software tools (particularly encryption technologies);
3. Increasing ease of launching automated cyberattacks;
4. Rapid development of novel cybercrime techniques;
5. Rapid nature of cyberattacks;
6. Fragility and temporal nature of electronic data;
7. Lack of investigative capacity devoted to cyberspace;
8. Increasing reliance on (initial) automated investigation processes due to increasing number of internet users;
9. Decentralized nature, architecture, and design of the internet;
10. Multi-jurisdictionally of the crimes; and
11. Anonymous nature of online communications.

II. Challenges to Developing Legal Frameworks

Beyond the general challenges faced in combatting cybercrime, there are challenges in **(A)** adapting current legal frameworks and **(B)** developing new, cybercrime-specific aspects and legal frameworks, while also **(C)** respecting constitutional limits.

A. Adapting Current Legal Frameworks

Developing cybercrime countermeasures requires building a sufficiently robust and flexible legal framework through legislative and regulatory action. That framework needs to provide law enforcement agencies with both procedural means and actual resources to fight cybercrime.[3] Adapting pre-existing legislation that has not been specifically intended to deal with cybercrime often may be an option, even if not ideal. For example, in the United States anti-money-laundering (AML) and identity theft laws are being applied to their cyberspace analogs.[4] Many other countries have adapted existing legislation by introducing provisions that extend existing laws to include criminal activity conducted on the internet or facilitated by the use of ICT. Short of legislative activity, the application of existing laws[5] and concepts[6] to cyberspace is dependent upon judicial interpretation of creative prosecutions; just how the prosecutors and the judiciary act, and interact, will be shaped by a country's legal system, especially whether it is in the civil or common law approach, in the determination of essential values and overall policy.[7]

Technological developments present perennial challenge for combatting cybercrime. One that, though only nascent at best, deserves raising is the development of AI as combined with the creation of autonomous systems. It is not all that far in the future that one could foresee such systems being on such a level of sophistication that they are less "tools" and more as cognitive "minds". For the purposes of the Toolkit, such advances have a particular potential bearing on understandings of criminal liability. As discussed further on, criminal liability requires two criminal components be satisfied: first, an objective, fact-based showing of an action, or *actus reas,* and, second, the accompanying, requisite mental state, or *mens rea* ("guilty mind"), which requires a subjective determination (*see* sections 1 D and 4 A, below). It is not inconceivable that AI could "commit" crimes in their own right, therein complicating mens rea assessments.[8] Although AI is not presently subject to criminal liability, considering how it might be addressed should be borne in mind by governments—indeed, one model for doing as much might, for instance, be borrowed, from criminal liability of corporations.

Case 1.4: United States v. Liberty Reserve (USA)[9]

Incorporated in 2006 in Costa Rica, Liberty Reserve was a centralized, digital currency service that operated its own currency exchange using a digital currency, commonly called the "LR". The exchange allowed the anonymous transfer of client funds between third party payment exchange merchants and bank accounts. Liberty Reserve allowed clients to create

layered anonymity because of exceptionally lax identification requirements. Furthermore, they worked with unregulated money service businesses that operated using equally lax identification requirements. In doing so, Liberty Reserve charged fees for services rendered to clients, including currency exchanges and money transfers. Liberty Reserve became an ideal method for laundering and transferring monies internationally, with over US$6 billion were allegedly laundered through its channels.

On 28 May 2013, prosecutors in the US Southern District of New York brought charges against seven individuals under the USA PATRIOT Act for money laundering and running an unlicensed financial transaction company. The provisions used to target those at Liberty Reserve were not specifically targeting cybercrime.[10] The investigation involved operations in at least seventeen countries.

This case is indicative both of the ease with which financial cybercrimes can be committed thanks to the connectivity of cyberspace, as well as the potentially very great financial gains that might be had from such crimes.

B. Developing Developing Legal Frameworks

Despite a wide range of efforts to create a favorable legal environment to tackle cybercrime, challenges persist to assuring adequate legal frameworks.

These challenges include, among others, difficulties in:

1. Drafting new and clear[11] cybercrime legislation after the recognition of an abuse of new technology and identification of criminal law gaps;
2. Developing procedures for e-evidence;
3. Ensuring the criminalization of new and developing types of internet crimes;
4. Introducing new investigative instruments in response to offenders' growing use of ICTs to prepare and execute their offences;
5. Promoting technologically neutral laws[12]; and
6. Balancing security and rights.[13]

Box 1.1: Computer-facilitated Fraud Involving Illegally-obtained Online Game Items[14]

Through mobile phones with a built-in SIM card, and thus access to gamers' IDs, Defendants would use stored credit to repeatedly and fraudulently purchase game products from the

acquired phones. Thereafter, the game items would be sold for money on an intermediary trading website.

The Supreme Court of Korea read "game items" into the Game Industry Promotion Act: the "tangible and intangible results obtained through the use of game products [are] forbidden to make a business of exchanging such items".[15] The Court validated its position by looking to two different Enforcement Decrees for the Game Industry Promotion Act: first, the current Decree reads that "Game money or data, such as items, produced or acquired by using game products with personal information of another person"[16]; second, the former Decree read, "Game money or data, such as game items, produced or acquired by abnormal use of game products".[17]

Thus, Korea has used both amendments and judicial interpretation to ensure that evolving forms of cybercrime remain criminalized.

While countries are finding various means to criminalize the growing diversity of cybercrime, doubt has been expressed over the deterrent effect of current regulations.[18] Part of the concern is cybercrime's ubiquity and difficulties in identifying perpetrators and cross-jurisdictional prosecution.[19] Additionally, however, is the concern that penalties are not sufficiently severe to deter criminal behavior.[20] That said, anecdotal evidence suggests that this situation might be changing.

Case 1.5: United States v. Albert Gonzalez (USA)[21]

On 25 March 2010, Albert Gonzalez, the so-called TJX hacker, was sentenced to twenty years in prison, the longest US prison term in history for hacking.[22] Gonzalez engineered what was at the time the largest theft of credit and debit card information in US history (some eighty gigabytes of data), which resulted in the theft of over 130 million card numbers and costing individuals, companies and banks, and which amounted to nearly US$200 million in losses.[23] The hacks involved the first known intrusions involving decryption of PIN codes, a key protective feature in bank card security in the United States.

The sentence represents one of the toughest verdicts for both financial crimes and cybercrimes to date in the United States.[24] Although sentences have been becoming increasingly robust, they have not played a significant role in reducing cybercrime due to difficulties in identifying, arresting and prosecuting offenders. Also, restitution orders are rarely, if ever, fully paid back.[25]

III. Challenges of Additional Resources

Before defining the term of cybercrime,[26] it bears noting that **(A)** there are additional, noncriminal legal tools in preventing crime, **(B)** consumer awareness plays a role in preventing crime and **(C)** government efforts to combat cybercrime will have to involve public-private partnerships due to the important role of nonstate actors in the provision of infrastructure and cyber services Another, separate challenge is faced in **(D)** developing sufficient capacity to detect cybercriminal activities.

A. Additional Legal Tools

Criminalization is not the only option to combatting untoward cyber activity. Indeed, pursuant to the *ultima ratio* principle,[27] criminal law should be used only as a last resort for dealing with a social ill. Both administrative and civil measures might be taken to combat errant cyber activity. Administrative measures that might be taken include ordering the removal of certain content, or the "closing down" of offensive websites (for instance, in combatting child pornography).[28] Ordering an ISP to block access to the website might also be an option,[29] although, as discussed further on, the internet's transnationality limits the efficacy of such options. Removal of content and closing of websites may also interfere with domestic or foreign criminal investigations (or national security investigations), or such measures may hinder efforts to rescue trafficking victims if carried out without coordination. Additionally, many legal systems allow individual victims redress for damages in civil courts. Due to the cost and complexity, as well as shifting the burden from the state to the victim, civil sanctions are largely unused, except in the case of copyright violations.[30] Other tools include the creation of a digital ID—for instance, in South Korea, these IDs, which are visible to law enforcement but not to the public, have helped to reduce incidences of cyberstalking and cyberbullying.

B. The Consumer's Role

What roles and responsibilities do individuals have in combatting cybercrime?

A growing body of literature recognizes the responsibilities of individuals to ensure they take proper precautions to secure their devices and data.[31] As certain cybercrimes could be easily prevented through user caution and awareness, it has been argued that the user ought to be incentivized by the law to do so. Basic steps include using and maintaining up-to-date antiviral software, keeping personal devices clean of malware, maintaining up-to-date antiviral software, being mindful when opening emails and downloading files and being conscious of sharing personal information. Additional techniques include the use of strong passwords, two-step verification, personal identification numbers (PINs), encrypted communications, as well as keeping device Bluetooth and WiFi off when not in use. In many instances, virtual private networks (VPNs), which connect users to

a server, therein giving the appearance that the traffic is coming out of that source rather than from the user, might be used to improve privacy. By failing to take simple security actions, the user not only becomes a vulnerable target but also allows criminals to coopt electronic devices to conduct other malicious and criminal behavior, costs which are potentially both considerable and which are passed on to society.[32] However, while many countries encourage the use of appropriate protection, only a few go so far as to sanction failure to use protection.[33]

Of greater concern than the role of the individual is the role of the private sector companies involved or operating critical infrastructure. Companies—frequently driven almost-exclusively by profit in the age of privatization—have proven themselves slow to invest the necessary resources in many aspects but quite notably in the area of industrial controls and security.[34] Indeed, Kaspersky Labs found critical infrastructure companies still running 30-year-old operating systems.[35] In the United States, attempts to legislate requiring companies to maintain better security practices were stymied on the grounds that it would be too costly for businesses.[36] Such infrastructural lacks have been aggravated by user apathy, with many companies operating industrial control systems not even changing the default passwords.[37]

C. Private Sector Cooperation

The ease and speed of information-sharing between cybercriminals, and the disparateness of criminal activity, makes it difficult for either law enforcement or targets to keep up. As discussed in the previous section in greater depth (*see* section 1 B, above), cybercrime cannot be effectively combatted without cooperation between the public and private sectors.[38] As cyberspace continues to develop, different investigative tools will be required of law enforcement, as dramatically shown in the FBI's inability to independently unlock iPhone.[39] Only partnerships with the private sector will make such possible.

Box 1.2: WannaCry Ransomware Attack

In May 2017, a huge cyberattack—described by Europol chief as "unprecedented in its scale"—affected more than 200,000 victims in over 150 countries.[40] While the United Kingdom and Russia were the worst affected, the attack was global in nature, with large affected institutions including the UK's National Health Service, Russia's Interior Ministry, Germany's rail network Deutsche Bahn, France's car manufacturer Renault, Spain's telecommunications operator Telefonica and US logistics giant FedEx.

The virus, a worm-application, was paired with ransomware that takes control of users' files and demands payments of US$300 in Bitcoin in order to unlock files and return control to users. What made this malware—having permutations on the name WannaCry and WannaCrypt—particularly virulent was its ability to move around a network by itself,

spreading itself within networks without relying on human activity to spread it.[41] The attack was indiscriminate rather than targeted, with evidence suggesting a North Korean connection.[42]

The initial attacks were hindered by a 22-year-old UK security researcher—going by the name of MalwareTech for purposes of anonymity—who discovered an apparently unintentional "kill switch" to the malware.[43] However, due to the relative ease of launching cyberattacks, and the great deal of money at stake, concerns persist that either attacks will be relaunched with the coded kill switch removed, or that subsequent attackers will learn from lessons from this experience.[44]

WannaCry is a weaponization of one of a series of system's vulnerabilities first identified by the US National Security Agency (NSA),[45] and which were stolen when the NSA was hacked[46] and then leaked to the public in April 2017.[47] Of that cache, it is the tool codenamed "EternalBlue" that appears to have been "the most significant factor" behind the WannaCry attack.[48] Among other things, the attacks have reignited the debate over whether governments should disclose web or system vulnerabilities of which they become aware.[49]

The cyberattacks highlight the importance of user awareness. WannaCry appears to have capitalized upon outdated systems for which patches existed, and even to have targeted systems and sectors that might tend to run on legacy systems, such as healthcare and transport. The attacks emphasize that it is incumbent upon users—individual and institutional—to keep their systems up to date by installing the fixes—so-called "patches"—that developers, such as Microsoft or Apple, make available as they become aware of system weaknesses.[51] In this instance, the attacks capitalized vulnerabilities in outdated Microsoft Window software; Microsoft had released security updates to patch this matter in April, and, responding to the attack, did so again on the day of this attack.[52]

As ransomware attacks grew by fifty-one percent last year,[53] the threat seems unlikely to abate. "This [problem] is one in which what's broken is the system by which we fix", said Professor Zeynep Tufeki of the University of North Carolina.[54]

D. Detecting Cybercrime

Detecting cybercrimes is challenging because, first, the victim may have no idea that a crime has occurred, and, second, cybercriminals are wont to operate behind multiple layers of fake identities and often operate out of nation-states having either limited cybercrime-fighting capacity, or limited interested in taking on such a fight.[54] It is generally difficult to detect system security breaches before any visible damage—such as the fraudulent transferring of a victim's funds—has been done. Moreover, much of the damage can be done simply by surveilling—for instance, in the collection of personal information or metadata for use in identity theft. Moreover, even where a breach has been identified, hackers often hide their identities through the use of various tools. Further difficulties

arise where "acts that might previously have been considered civilian attacks are […] uncovered as acts of states against states via nonstate actor proxies".[56]

Encryption is also an issue. Data can be increasingly stored and sent in an encrypted form. Of particular note is end-to-end encryption (E2EE), which is becoming increasingly common, if not quite (yet) the norm.[57] With traditional encryption methods, the facilitator—that is, the company, transmitter or ISP—itself holds the cryptographic key. As a result, anyone compromising the facilitator's systems has access to the cryptographic key, and thus to the data of all individual users relying on the facilitator's resources. By contrast, E2EE securitizes communications on an individual basis. E2EE creates two complementary cryptographic keys (rather than one, common key, as is in traditional encryption). Those keys are with the communicating parties and the communicating parties alone[58]: the decryption key (a "private" or "secret" key) never leaves the user's device, while the encryption key (a "public" key) can be shared with those sending messages to the user.[59] With this protection in place, only those directly communicating can read the messages, thereby preventing even successful eavesdroppers from understanding the message's garbled contents.

Successful eavesdroppers would be forced to independently decrypt the data. However, the possibility of independently decrypting captured E2EE-protected data is increasingly unlikely, as the possible number of decryption combinations has increased exponentially. Indeed, the possibility of cracking an encrypted message—typically done through a cryptanalytic attack, known as a brute-force attack or an exhaustive key search—has become challenging to the point of near-impossibility, even with sophisticated software.[60] Although E2EE is still susceptible to so-called man-in-the-middle attacks (whereby the interceptor impersonates the recipient, attempting to encrypt the message with his public key instead of the one intended by the sender), E2EE has substantially reduced the viability of illegally intercepting data.[61] Deciphering by interlopers is made more difficult by features such as PFS-perfect forward secrecy, which create new encryption keys for each message sent.[62] As a result, intercepting data being sent between devices is generally less valuable than being able to read the data on the device, either before encrypting and sending or after receiving and decrypting.

Box 1.3: Understanding Encryption

Encryption methods are rendering it increasingly difficult for those intercepting data to decipher the data.[63] For instance, the factorization of a 256-bit AES key[64]—which the NSA requires for data classified up to Top Secret, and which is used by many other third-party providers, including WhatsApp—has 256-bit possible options: that is, any sequence of 256 bits is a potential key, and there is no internal structure to those 256 bits.[65]

One byte—equivalent to two nibbles or eight bits—can hold 256 different states, possibilities or values. Each bit has one of two values: 0 or 1. The number combination exponentially increases the number of potential sequences.

For example, there are sixteen possible key combinations for a 4-bit sequence:

0000 → 0,	0100 → 4,	1000 → 8,	1100 → 12,
0001 → 1,	0101 → 5,	1001 → 9,	1101 → 13,
0010 → 2,	0110 → 6,	1010 → 10,	1110 → 14,
0011 → 3,	0110 → 7,	1011 → 11,	1111 → 15.

The above assessment is based on a binary computing; however, quantum computing, which uses "quibits" instead of bits, would transform binary form into a multidimensional manner (*see* section 2 A, below). Steady improvements in computer power have resulted in the periodic increasing in the length of number-based keys, meaning that encryption has a shelf life and is rapidly becoming more vulnerable. Quantum computing is set to disrupt present understandings and significantly complicate matters. Quantum communication embeds the encryption key not in code but in photons (that is, particles of light). In addition to dramatically heightening system security, the so-called "quantum key distribution" means that interception by would-be hackers necessarily alters or destroys the particles of light, making any attempt at hacking immediately noticeable.[66]

Critics have claimed that E2EE plays potential havoc with investigations by law enforcement, as even third parties involved in transmitting messages—telecom companies, ISPs, the application administrators and the sort—do not have anything more than the garbled, encrypted data, and thus, are no more capable of understanding communications than are any eavesdroppers. Such technological compromises have led law enforcement to press IT companies to design so-called "back doors" that would allow the reading of communications. Many companies boast using E2EE, with WhatsApp perhaps being the most visible of late.[67] The flipside of these developments is that governments sometimes restrict the key size that apps may use. For instance, India restricts ISPs and TSPs to 40-bit key length (relatively low security).[68]

Encryption techniques are becoming increasingly complex. One of particular note is that of the "one-time pad" (OTP), which relies the exchange of a one-time, truly random, never reused (neither in part or in whole) pre-shared key that is at least as long as the message that has been sent.[69] It has been argued that such encryption algorithms would create mathematically "unbreakable" ciphertexts. Be that as it may, practical problems and limitations have prevented OTPs from becoming widely used.

IV. Challenges to International Interoperability

In a world of increasing transnational conduct, improving **(A)** international cooperation and addressing **(B)** jurisdictional and conflict of laws issues are paramount to facilitating international interoperability of frameworks developed to combat cybercrime.

A. International Cooperation

As cybercrime defies traditional notions of geography and mobility, traditional definitions of jurisdiction have become insufficient. As discussed further on, various efforts have been undertaken to mitigate harder, limiting notions of jurisdiction (*see* sections 2 E and 3 A, below). Certain international legal instruments have been influential in harmonizing legislation.[70] European instruments have been particularly impactful on national legislations, especially the CoE Convention on Cybercrime (commonly known as the "Budapest Convention"),[71] which has had an impact on legislation even in those states that have not ratified it; the European Council Framework Decision 2005/222/JHA on attacks against information systems[72]; and European Council Framework Decision 2004/68/JHA on the sexual exploitation of children and child pornography.[73] The EU Data Retention Directive 2006/24/CE[74] has also had a great impact; however, on 8 April 2014, the Court of Justice of the European Union (CJEU) declared the Directive invalid in response to a case brought against Irish authorities.[75]

In general, there has been a remarkable degree of convergence of various multilateral instruments on cybercrime in criminalizing acts against the confidentiality, integrity and availability of computer data and systems. In addition to the aforementioned European measures, multilateral instruments connected with the African Union (AU), the League of Arab States(Arab League), the Economic Community of West African States (ECOWAS), the Common Market for Eastern and Southern Africa (COMESA), the Commonwealth Secretariat (COMSEC) and the International Telecommunications Union (ITU) all criminalize illegal access to: a computer system, illegal interception, illegal computer data and system interference and the misuse of devices.[76]

On the other hand, other offences, such as illegally remaining in a computer system to date, have received considerably less support.

Remarkably, identity theft has not been universally condemned in multilateral instruments, nor have extortion, spam, harassment, stalking or bullying.[77] Other areas receiving little demand to be classified as crimes in international treaties include:

- Violation of data protection measures for personal information;
- Breach of confidentiality;
- Use of forged or fraudulently obtained data;
- Illicit use of electronic payment tools;
- Acts against privacy; disclosure of details of an investigation; and
- Failure to permit assistance.[78]

When it comes to computer-related acts, two categories—forgery and fraud—are widely criminalized, although neither the CIS nor the COMSEC have criminalized such actions. Computer solicitation or grooming of children has been included only in the CoE Convention on Protection of Children against Sexual Exploitation and Sexual Abuse (the "Lanzarote Convention"),[79] the first

international treaty that addresses child sexual abuse that occurs within the home or family.

As to computer content-related acts, the most frequently criminalized acts are those involving child pornography and, to a lesser extent, dissemination of racist and xenophobic materials and related threats and insults.[80] Genocide, terrorism, pornography (including facilitating access of a child to pornography), gambling, money laundering and illicit trafficking using electronic media technologies have been very rarely criminalized as cybercrime to date.[81]

Addressing a very specific form of crime via a treaty may not, however, be advisable:

1. First, of course, countries are free to criminalize whatever conduct they see fit, whether or not a treaty exists.
2. Second, since treaties are relatively inflexible, countries may wish to wait to see if a crime trend persists and is serious or to discern how best to frame a criminal provision. Importantly, many of the crimes above may be addressed by a non-cybercrime treaty (genocide, terrorism, etc.) or by a cybercrime treaty or domestic statute in a different guise (acts against privacy may be covered by illegal access; extortion may be covered by an ordinary criminal statute; illicit use of electronic payment tools may be covered by misuse or possession of access devices; etc.)
3. Finally, crimes that are defined more generally will often be easier to prosecute and prove because they demand fewer specific elements.

International cooperation, essential for effective cybercrime prevention and prosecution, has been largely supported by the international community. One such example is Operation Blue Amber, which, in a series of international actions, tackled organized crime in various locations across the world (*see* box 1.4, below).[82]

Having said as much, several individual countries have already criminalized many of the aforementioned behaviors. On the other hand, ratification of treaties is frequently predicated on "Reservations", whereby ratifying countries decline to accept one or more of the treaty's clauses, or whereby the treaty's implementation is subordinated to domestic law.[83] Such reservations are most typically used to assert that the treaty is limited to the state's constitutional interpretation, or for where the treaty will be made subject to domestic enabling legislation that places limits on treaty applicability and enforcement. While the number of ratifications may give the mistaken impression of widespread acceptance and enforcement, Reservations can effectively gut a treaty of its most important provisions. It is for this reason that the Budapest Convention strictly limits the Reservations that may be taken.[84]

Box 1.4: Operation Blue Amber

Police arrested 130 suspects in connection with cyberfraud, including fraudulent online purchases of airline tickets using stolen credit card data at 140 airports around the world in

an international law enforcement operation. The operation was coordinated through Europol in The Hague, the Netherlands, INTERPOL in Singapore and Ameripol in Bogota, Columbia with support from Canadian and US law enforcement authorities. Increased commitment from law enforcement agencies, private sector and international organizations enabled the operation to be conducted at airports in twenty-five countries in Europe and twenty-four other countries in Asia, Australia, America and Africa.

The operation against airline fraudsters is part of Operation Blue Amber, a series of international actions tackling organized crime in various locations across the world. Europol said it will continue to support EU Member States, working closely with the private sector and other international organizations, to improve security at the airports by fighting this type of online fraud.

B. Jurisdictional Challenges

As already mentioned, jurisdictional and cooperation issues frequently hinder investigation and prosecution.[85] Law enforcement agencies are usually jurisdictionally restricted and therefore rely on foreign agencies or international agreements to pursue multinational cybercriminals and prosecute them.[86] This problem is exacerbated in comparison to traditional crimes largely due to the transnational nature of not just the cyberspace but also of various internet actors, especially ISPs.[87]

Procedures for international cooperation also create obstacles. Extradition, mutual assistance, mutual assistance for provisional measures, trans-border access to stored computer data and communication networks for investigations are all problematic areas. Non-participation in cross-jurisdictional information sharing agreements has far reaching consequences. For example, not being party to such an agreement may limit the ability of authorities to retrieve information and metadata, such as on cyberattacks their nature, extent and trend. Such difficulties are especially evident when the servers are physically located in foreign jurisdictions with either rigid or nonexistent laws.[88]

Case 1.6: United States v. Aleksandr Andreevich Panin ("SpyEye")[89]

SpyEye is a prolific type of Trojan malware that is estimated to have infected more than 1.4 million computers, resulting in losses of at least US$5 million between 2009 and 2011. SpyEye was developed by Aleksandr Panin, a Russian programmer who was the primary developer and malware distributor, and Hamza Bendelladj, an Algerian hacker.

"One of the most professional and successful malware families", SpyEye even offered buyers regular version updates and betas.[90] The SpyEye code operated by secretly infecting victims' devices, enabling cybercriminals to remotely control those devices through so-called

command and control (C2) servers.[91] SpyEye could be tailored to obtain victims' personal and financial information, with version of the software being sold—on an invite-only basis—for between $1000 and $8500 to at least 150 clients. Ultimately, Defendants sold SpyEye to an undercover FBI agent.[92]

US authorities indicted Defendants on the grounds of the impact of SpyEye on US interests and on the presence of a control hub in Georgia, and sought extradition for criminal proceedings. For a period of years, Defendants were tracked by a consortium of law enforcement agencies (UK, US, Thai, Dutch, Dominican, Bulgarian, Australian), as aided by several private sector entities (Trend Micro, Dell Secureworks, Trusteer, Underworld.no), and supported by INTERPOL. Following the arrests of Panin and Bendelladj in the Dominican Republic and Thailand, respectively, Defendants were transported to the United States for trial.[93] Both pled guilty and were sentenced to a combined twenty-four years and six months in prison.[94]

The SpyEye case shows the multinational nature of cybercrime and the barriers hindering prosecution. Notably, the absence of a formal extradition agreement between Russia and the United States, along with jurisdictional issues, caused substantial hindrance. On the other hand, the case also illustrates the potential that cooperation and partnerships—both on the international level and between the public and private sectors—can have.[95]

V. Safeguards

Building cyberspace requires attention to implementing the necessary safeguards. Fundamentally, **(A)** legal limits, notably constitutional and human rights laws,[96] must be respected even as appropriate security is implemented. With that in mind, safeguards can be developed to protect **(B)** both the environment of cyberspace itself by protecting against excessive data collection, as well as by protecting users and their data. Attention must be given to protecting the basic interests of users as members of society by assuring **(C)** the constituent parts of freedom of communication, namely, freedom of opinion and expression and freedom of information.

A. Respecting Constitutional Limits

Although discussed in greater depth in section 4 A, specific mention needs to be made to preserving and respecting constitutional guarantees and limits in this context, namely the challenges of developing legal frameworks.[97]

Any criminalization of communications in cyberspace is potentially in conflict with freedom of expression, a constitutional right in most countries, as well as being a limit on both the freedoms of

the press and of artistic expression.[98] Infringements of these basic rights are permissible only if they are proportionate to the danger that they seek to combat.[99] Some countries have constitutionalized the so-called "harm principle",[100] which more generally limits the scope of the criminal law to conduct that is harmful or imminently dangerous to an interest worthy of protection.[101] Many of the limits placed on state action to secure cyberspace exist and are supported in international law, which is binding law on States Parties (*see* section 5 A, below).

It should be born in mind that criminal law generally requires not only a guilty act ("*actus reus*") but a concurrently guilty mental state ("*mens rea*") for culpability to attach (*see* section 1 D, above),.[102] Such elements of the crime also must be respected in cybercriminal prosecutions (*see* section 2 A, below).

B. Balancing Data Collection with Data Protection

For cyberspace to remain open and free, the same norms, principles and values that are upheld offline must apply online. Fundamental rights and the rule of law need to be protected in cyberspace. Data protection is about safeguarding the fundamental right to privacy, a right enshrined in numerous international and regional instruments. However, according to the United Nations Conference on Trade and Development (UNCTAD), only 107 countries had privacy laws or bills in place as of 2014.[103] Other countries have privacy laws governing select areas—for example, children or financial records—but not a comprehensive law.[104]

Data collection is commonly understood as securing any personal information that is automatically collected, processed and stored. It is essential that data protection laws restrain and shape data collection, managing and storage activities conducted by both companies and governments. Past behavior shows that, unless restrictive rules are in place, both public and private sector entities will collect, mine and store as much information as possible without necessarily even informing the public of such activities.[105]

Our freedoms and prosperity increasingly depend on a robust and innovative internet, which will continue to flourish if private sector innovation and civil society drive its growth. But freedom online requires safety and security too. Cyberspace should be protected from incidents, malicious activities and misuse.

Governments have several tasks *vis-à-vis* cyberspace:

- To safeguard access and openness;
- To respect and protect fundamental rights online; and
- To maintain the reliability and interoperability of the internet.

As discussed, because the private sector owns and operates significant parts of the infrastructure creating cyberspace, any initiative addressing data collection and protection should engage with the private sector.

C. Freedom of Communication

As discussed in greater depth further on (*see* section 5 A, below), freedom of communication relies on two complementary rights: **(1)** the freedom of opinion and expression, which is the fundamental right to feel, think and believe and to express oneself, and **(2)** the freedom of information, which is a fundamental prerequisite to allowing the creation of full and informed opinions and allowing self-expression.

1. Freedom of Opinion and Expression

Freedom of opinion and expression is a fundamental right, declared in a number of instruments, including in the Universal Declaration of Human Rights (1948),[106] the International Covenant on Civil and Political Rights (1966)[107] and the American Convention on Human Rights (1969).[108]

The internet has been revolutionary in many ways but especially in terms of facilitating communication and freedom of expression. The internet has significantly expanded the meaning of that right, allowing instant, inexpensive communication to almost everyone, dramatically impacting journalism, access to information and knowledge sharing and ideation.[109] Nevertheless, freedom of opinion and expression has been suppressed in countries for various reasons including public safety, breach of confidentiality, defamation, threats to person or property, terrorism, incitement to genocide, incitement to religious hatred and child pornography.[110]

The internet's configuration and architecture have greatly impacted the flow of information, as well as what level of control can be exerted over it. First developed by the US military as part of the Pentagon's Advanced Research Projects Agency Network (or "Arpanet") program to create a command and communication contingency in the midst of war,[111] the internet was developed to be flexible, decentralized, open and neutral. That architecture, which has fostered for rapid growth and amazing creativity, should be preserved. As such, any regulations should be designed in dialogue with all stakeholders and, fundamentally, should seek to maintain the basic characteristics of democratization, universality and nondiscriminatory access.

Efforts should be made to assure that the special characteristics that have made the internet a rich medium for growing democratic, open, plural and expansive exercising of expression are protected. Such an understanding has been recognized at the international level: jointly, the UN Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Cooperation in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information have recognized that "[a]pproaches to regulation developed for other means of communication—such as telephony or broadcasting—cannot simply be transferred to the internet but, rather, need to be specifically designed for it".[112]

The UN Human Rights Council in 2012 declared that freedom of expression on the internet is a basic human right and affirmed that people have the same rights online that they have offline.[113] That view was reaffirmed in 2016 regarding the importance of promoting, protecting and enjoying human rights on the internet, including privacy and freedom of expression.[114]

2. Freedom of Information

Access to, or freedom of, information (FOI), or the right to information, is a corollary to freedom of expression that looks to inform the citizenry on government action. It is the right to access information held by public bodies, and includes the right to seek, receive and impart information and ideas. The UN General Assembly, in its very first session in 1946, recognized it as essential to the underpinning of democracy, adopting a resolution stating that "Freedom of information is a fundamental human right[, …] the touchstone of all the freedoms to which the United Nations is consecrated."[115]

Elaborating on this statement, the UN Special Rapporteur on Freedom of Opinion and Expression had the following to say:

> "Freedom will be bereft of all effectiveness if the people have no access to information. Access to information is basic to the democratic way of life. The tendency to withhold information from the people at large is therefore to be strongly checked."[116]

Functional polities rely on civic participation and on individuals being able access to information held by various public bodies; that information allows individuals to be aware of, involved in and responsive to public activities. Such information ranges from interpretations of applicable laws to details on economic, social, or public concerns. A central tenet to the rule of law[117]—the notion that all, including the government, are subject to the law[118]—, access to information makes transparency, accountability and participation—the so-called TAP principles—possible. In addition to being key tools for combatting corruption, the TAP principles increase government efficiency and responsiveness, and build civic trust.[119] Accessing public information is not only a right of every person but also necessary to making informed decisions and to living an autonomous life.[120] It bears noting that right is not absolute and that freedom of information may need to be limited in certain instances, such the public interest.[121]

Access to information legislation should reflect the fundamental premise that all information held by governments and governmental institutions is in principle public and may only be exceptionally withheld, such as for reasons of privacy or security. There is a global trend to recognize the right to information, and, since 1990, the number of countries with such legislation has grown from thirteen to ninety-five.[122]

Conclusion

This subchapter has given an overview of challenges facing law enforcement in combatting cybercrime. Those challenges come in all forms, ranging from the basic and general—yet perfidious—challenges associated with the nature of ICT and the development of cyberspace, to challenges in developing legal frameworks that both respect exist existing legal frameworks and yet which can accommodate the diverse novelties of cyberspace. Public safety and security in the analog world is, as the WDR aptly notes, a public good which governments are obliged to ensure.[123] However, while it is a unique public good so much of the analog world—its data, communications and critical infrastructure—is controlled by the private sector or other nonstate actors.[124] Thus, beyond taking the traditional tacks of acting through policies, laws and institutions, governments must also seek additional resources, including informing consumers and engaging the private sector.

Having appropriately organized themselves, governments then face the challenge of assuring international interoperability. Jurisdictional and international cooperation issues create substantial difficulties to investigating and prosecuting multinational cybercrime cases. Moreover, challenges of certain states operating under insufficiently cybercrime-specific legal frameworks often hinders combatting transnational acts.

D. Framework for a Capacity-building Program

Table of Contents

Introduction

Capacity-building programs require resources. Although many sectors are competing for scarce resources, there is increasing recognition that at least some of those resources are urgently needed to combat cybercrime. There are several reasons for building such capacity—and just as many ways that capacity can be built. The Toolkit at large, and its Assessment Tool in particular (*see* section 7, below), aim to provide evidence and direction for implementing targeted capacity building. At a high level, some of the main reasons for allocating scarce resources to cybercrime capacity-building programs include the following:

- **Societies are increasingly reliant on ICT.** As discussed (*see* sections 1 A and 1 B, above), society *writ large* is increasingly reliant on ICT for all manner of activities, and ICTs are used in support of all manner of ventures, both public and private. Many have become dependent on the existence of ICT in their day-to-day lives. Every region of the world has experienced massive growth in internet usage,[1] largely facilitated by the increased availability of broadband connections and the growing use of internet-enabled mobile phones and related applications.[2] That growth has created spaces for all sorts of development—both economic and commercial, as well as individual and social. As such, ensuring the security of, and confidence and trust in, ICTs and ICT systems should be a priority of any government.
- **e-Evidence's ubiquity in all crime-types.** Cybercrime is no longer a peripheral phenomenon. The more ICTs are used, the more criminals seek to exploit corresponding—and ever-developing—vulnerabilities. As the division between crimes occurring in the "cyber" world and those in the "real" one continues to blur,[3] ICTs are increasingly holding evidence, direct

or tangential, that is relevant not only to cybercrime but to any crime.[4] Thus, regardless of the matter, law enforcement officers, prosecutors and judges are already frequently confronted with e-evidence; such is the case not only in criminal matters but also in commercial, civil, labor and other matters. Capacity-building programs can help criminal justice authorities to meet these challenges, for example, through training and institution-building and by mainstreaming the issues of cybercrime and e-evidence into law enforcement and judicial training curricula.

- **Cybercrime capacity-building programs improve rule of law and civil and human rights safeguards.** Many governments are adopting cybersecurity strategies with the primary purpose of protecting critical information infrastructure. Capacity-building programs on cybercrime can support a crucial element of cybersecurity strategies, especially responding to attacks against the confidentiality and integrity of ICT systems and services. Such programs can also help governments meet their positive obligation to protect people from all types of crime, including murder, human trafficking, sexual violence and other types of violent crime, as well as fraud, corruption, drug trafficking, extortion, stalking or theft (*see* section 1 B, above). When governments take action against cybercrime they must respect rule of law and civil and human rights requirements. Investigative powers must be limited by conditions and safeguards.[5] The preservation, analysis and presentation of e-evidence must follow clear rules to serve as evidence in court. Strengthening the focus on the criminal justice response to cyberattacks may help improve both rule of law and civil and human rights safeguards,[6] both at large and with regard to cyberspace. Correspondingly, capacity-building programs should furthermore strengthen regulations and mechanisms for the protection of personal data, a dimension that is particularly important given that much of the most sensitive of personal data is nowadays stored in electronic form (*see* section 2 D, below). In short, such programs not only protect people against crime but also protect their rights.
- **Cybercrime capacity-building programs facilitate human development and improve governance.** ICTs can be "powerful tools for human development and poverty reduction", something that cybercrime capacity-building programs might help societies realize.[7] Relatedly, strengthening confidence, trust, security and reliability of ICT and of ICT systems will facilitate economic development and access to education and sharing of information.[8] Effective criminal justice systems enhance the physical security and health of individuals, for example, by protecting children against sexual exploitation and abuse, by preventing the distribution of counterfeit and substandard medicines or by protecting people against crime in general. Increased adherence to rule of law contributes to democratic governance and reduces undue interference in individual rights.

I. Objectives of Cybercrime Capacity-building Programs

In promoting cybercrime capacity-building programs, it is important to begin by **(A)** understanding the rationale and objectives of such programs, and **(B)** using such programs as a "process of change" that may go well beyond cybercrime.

A. Rationale & Objectives

Cybercrime capacity-building programs generally focus on strengthening the response of criminal justice actors to various forms of cybercrime. Once a crime has been committed, ICT-stored-evidence must be preserved and protected (*see* section 2 C, below). Cybercrime and e-evidence are transversal and transnational challenges requiring cooperation at all levels: interagency, public/private (in particular law enforcement/internet service provider) and international cooperation. Strengthening these various avenues of cooperation should be reflected in the objectives of any capacity-building program.

B. Supporting a Process of Change

As with any other capacity-building program requiring technical cooperation, cybercrime capacity-building programs are implemented to support processes of change. To take effect, such processes, as well as their objectives and expected outcomes, must be not only defined but also "owned" by the institution receiving support. Doing so creates an institution-wide "culture", one which is exemplified by leadership from above and which is implemented at all levels.[9] Without commitment from the top to a clearly defined process of change, it will be difficult for the larger institutional "cultural" issues to take root.

For example, while *ad hoc* training courses for judges and prosecutors might well be beneficial to the participants, without a sustained effort, it may have limited impact on the system with temporary results. By contrast, a more holistic, sustained and longer-term approach is preferable. For example, such a sustained effort methodically develops a capacity-building program that begins by training trainers, piloting courses, including standardized training materials and integrating *curricula* across institutions having shared or related competencies for cybercrime.

Additionally, once a defined strategy is in place, donors can better coordinate their inputs in a complementary and more effective manner.

II. Elements of Capacity-building Programs

As described in sections 1 B and 1 C, above, cybercrime is a large and broad topic. Accordingly, capacity-building programs targeting cybercrime should be likewise encompassing. Areas of focus might include **(A)** elaborating cybercrime policies and strategies, **(B)** elaborating effective, cybercrime-specific legislation, **(C)** creating cybercrime specialized law enforcement units, **(D)** training government authorities and personnel in cybercrime matters, **(E)** encouraging cooperation between the public and private sectors and **(F)** furthering international cooperation.

A. Producing an Overarching Cybercrime Policy & Strategy

The basis for any good approach to cybercrime is the development of effective policies based on stakeholder consultations, and which include comprehensive strategies and actions plans.

Such policies, strategies and action plans might include the following elements:

1. **Engaged decision-makers.** It is essential that decision-makers in government and affected organizations understand both the varied risks and the corresponding options, and that they manage to agree on setting strategic priorities.

2. **Synergistic cybersecurity strategies.** Cybercrime and cybersecurity strategies are interrelated and mutually reinforcing. As such, synergies and links must be explicitly identified, ensuring coherence.

3. **Multi-stakeholder participation in strategy elaboration.** As cybercrime and cybersecurity implicate the entirety of society, part of the challenge in developing effective policies and strategies is ensuring the active participation of diverse stakeholders from both the public and private sectors.

4. **Approaches support human rights and rule of law requirements.** A criminal justice response to cybercrime implies a rule of law rationale; as such, rule of law requirements need to be respected and promoted as do general respect and promotion of human rights. As discussed (*see* section 4 A and 4 B, below), an appropriate balance between combatting crime and ensuring human-rights safeguards is central to the success of any strategy.

5. **Cybercrime strategies require vertical and horizontal management.** Once a cybercrime policy has been developed, the implementation of the ensuing cybercrime strategy begins. That implementation process is a complex one, involving many stakeholders and actors. Effective operationalization requires good management, both vertically and horizontally, clear information sharing and extensive coordination. The progress, results and impact must all be assessed in order to for any corrective measures to take effect, as well as to justify the allocation of resources.

6. **Concerted alignment of donor contributions and partner cooperation.** The development of a clear cybercrime policy, and subsequent implementation of the resulting cybercrime strategy, create a clear path for donors and other partners to provide support. Doing so will increasingly crystalize and clarify the anticipated change process that is desired. Moreover, encouraging such cooperation can lead to faster learning of lessons.

Many donors require that a policy be in place before approving technical assistance and undertaking capacity-building programs. That said, a program might be structured such that the development of a strategy on cybercrime is a central objective. For instance, CoE considers an official request for accession to the Budapest Convention to represent the government's commitment that in turn justifies capacity-building activities that would support the treaty's full implementation.[10]

B. Developing Cybercrime-specific Legislation

While cybercrime policies create the overall story, a central element to fighting any criminal activity must be based in the law. As such, criminal justice measures targeting cybercrime and e-evidence must be enshrined in the law. Also, while the responsibility for creating such legislation lies with public representatives and authorities, they should be supported by other stakeholders, public and private, in the appropriate tailoring, targeting and wording of any such legislation. Such legislation is a central part to furthering interoperability (*see* section 3 A, below).

Domestic cybercrime legislation would address the following areas:[11]

1. **Substantive law measures.** The central plank and basis of the law is the development of, on the one hand, what substantive legal rights and responsibilities surround a matter, and, on the other hand, what actions are disallowed. Substantive legal matters govern society's behavior, and include, for instance, not only what actions and activities are disallowed, but also what is the requisite mental state, or *mens rea*, a perpetrator must have in order to be found culpable (*see* section 1 C, above). While much of criminal law differentiates between "general" intent (that is, the aim to commit a prohibited act) and "specific" intent (that is, the aim to commit both a prohibited act and aim to cause a particular effect resulting from that act),[12] cybercrime generally does not, requiring general intent alone.[13]
2. **Procedural law tools.** Having laid out prescribed and prohibited behaviors, the law must carefully discuss and delineate the associate procedural aspects, which include the procedures for investigating crime and enforcing the substantive law. Procedural tools also largely govern what powers lie with the authorities.
3. **Safeguards.** Due to the increased pervasiveness of the cyberactivity in all areas of the physical world, attempts to regulate a person's comportment in cyberspace must be careful not to become excessively expansive and infringe on other rights. As such, any law combatting cybercrime must pay careful attention establishing appropriate safeguards and the conditions under and by which investigative powers might be exercised.
4. **International cooperation.** The developed legislation must not only be inward or domestic-looking, but should also include provisions for international cooperation. To this end, international conventions, notably the Budapest Convention, offer both substantial guidance and structure.[14]

C. Creating Specialized Cybercrime Units

The investigation of cybercrime and forensic analysis of e- evidence and the prosecution of cybercrime require specific skills (*see* section 2 D, below). Authorities—investigatory, prosecutorial, judicial and advisory—should be supported in the setting up or strengthening of units that offer specialized support. Relatedly, mechanisms for assuring feedback and information sharing among agencies and units must be developed.

Particular attention should be paid to assuring that there is sufficient expertise among law enforcement authorities. Particular points of interest include (1) police-type cybercrime or high-tech units with strategic and operational responsibilities, (2) prosecution-type cybercrime units and (3) most generally, developing computer forensic resources for other law enforcement agencies that may not be created with the goal of tackling cybercrime, by either embedding small specialized units within, or by creating separate structures, or, at minimum, by creating focal points and procedures for looping specialized units into matters, wherever appropriate. Because cybercrime is not a "siloed" area of concern, it should be expected that even non-specialized units will have to be able to utilize e-evidence in non-computer crime, physical-world cases. As such, while certain tasks will necessarily require handling by trained specialists, many impediments could be prophylactically overcome by having these specialized units disseminate their knowledge and skills to the entirety of their agencies; indeed, in many case, knowledge dissemination might merely entail spreading awareness.

Beyond the law enforcement authorities, the judiciary should also have a place of recourse for matters of cybercrime. However, unlike with law enforcement authorities, setting up specialized cybercrime courts is not a preferable solution because the near-ubiquity of e-evidence means that all judges will have to consider such matters, regardless of the nature of the case in question. Good practices have shown that a better first step is to train some judges, and to use those judges as focal points for acting as a resource and disseminating knowledge more widely.

More generally, it is important that interagency cooperation be facilitated and actively encouraged. Such a unifying and integrative element is essential, as, to be effective, cybercrime units must cooperate both with other police services (such as economic crime units, child protection units) and with other institutions (such as financial intelligence units, CIRTs).

Conclusion

To support cybersecurity is to support and increase society's ability to grow more robustly and more equitably. Cybercrime capacity-building is an essential element therein. And while resource-scarcity is a concern for all governments and institutions, it is generally—and increasingly—recognized that cybercrime capacity-building programs cannot be left unattended. Reasons for supporting cybercrime capacity-building include the great and growing reliance of society *writ large* on ICTs,

and the ubiquity of e-evidence in all crime-types; developing such capacity has the tangential benefits of improving rule of law and human rights safeguards, as well as bolstering civil rights at large, facilitating human development and improving governance.

Cybercrime capacity-building programs are intended to support change. To that end, there must be a "culture of change" which, though initiated at certain points, must extend throughout all branches government. It must be owned by those in positions of authority, and administered and implemented in a coherent, holistic manner, as opposed to in a spotty, *ad hoc* fashion.

Producing an effective cybercrime capacity-building program requires a diversity of elements. At a fundamental level, both an overarching cybercrime policy and a strategy for implementation must be developed. Doing so will engage decision-makers, create synergistic cybersecurity strategies, support human rights and rule of law requirements. To be effective, the policy must increase multi-stakeholder participation in strategy elaboration, and that strategy must be effectively managed in both a vertical and horizontal sense. Relatedly, contributions by donors and cooperation with partners must align with that strategy in a concerted manner.

That overall cybercrime policy and implementation strategy should be embodied in cybercrime-specific legislation. Although applicable to all aspects of cybersecurity, such is particularly true for the criminal aspects. Doing so requires the development and legislating of substantive law measures, building of procedural law tools, the creation of safeguards for rights and the opening up of a national system into one that not only allows for but which facilitates international cooperation.

Lastly, cybercrime capacity-building programs can focus on creating specialized cybercrime units. Such units can, in turn, act to catalysts and educators in their own right, first, by taking on discrete cybersecurity activities, and, second, raising understanding and awareness among their peers and counterparts across all branches of government.

End Notes

Referenced in: § A. Purpose of Toolkit

1. "Infographic: McAfee Labs Threats Report," McAfee, (Mar. 2016), at https://www.mcafee.com/us/resources/misc/infographic-threats-report-mar-2016.pdf.
2. Jim Finkle, "SWIFT Discloses More Cyber-Thefts, Pressures Banks on Security," Reuters, (31 Aug. 2016), at http://www.reuters.com/article/us-cyber-heist-swift-idUSKCN11600C.
3. Vindu Goel & Nicole Perlroth, "Yahoo Says 1 Billion User Accounts Were Hacked," (14 Dec. 2016), at https://www.nytimes.com/2016/12/14/technology/yahoo-hack.html?mcubz=0.
4. UN Interregional Crime and Justice Research Institute (UNICRI), *Cybercrime: Risks for the Economy and Enterprises at the EU and Italian Level,* (Turin: UNICRI, 2014), at http://www.unicri.it/in_focus/files/Criminalita_informatica_inglese.pdf.
5. *Ibid.*
6. *Ibid.*
7. As discussed below, some acts that might otherwise constitute cybercrime, or that with the passage of time are revealed to be acts of states against states, and that might be characterized as cyberterrorism or cyberwarfare, are beyond the scope of this Toolkit.
8. *See* http://www.combattingcybercrime.org.
9. Unless otherwise indicated, such as in reference to a specific entity, the term "CIRT" will be used generically for all such related terms (*e.g.,* CERT, CSIRT).
10. World Bank, *World Development Report 2016: Digital Dividends,* (Washington: World Bank, 2016) [hereafter, "WDR"], at p. 222 *et seq.*, at http://documents.worldbank.org/curated/en/896971468194972881/pdf/102725-PUB-Replacement-PUBLIC.pdf.
11. *See, e.g.,* Nicole Perlroth, "Hackers Are Targeting Nuclear Facilities, Homeland Security Dept. and F.B.I. Say," New York Times, (6 Jul. 2017), at https://www.nytimes.com/2017/07/06/technology/nuclear-plant-hack-report.html?mcubz=0.
12. *See, e.g.,* "Warsaw Summit Communiqué, Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Warsaw 8–9 July 2016: Press Release (2016)," North Atlantic Treaty Organisation (NATO), (9 Jul. 2016) [hereafter, "Warsaw Summit Communiqué], para. 70, at http://www.nato.int/cps/en/natohq/official_texts_133169.htm.

Referenced in: § B. Phenomenon & Dimensions of Cybercrime

1. The title of this section owes its inspiration to ITU's report, International Telecommunication Union (ITU), *Understanding Cybercrime: Phenomena, Challenges and Legal Response,* (Geneva: ITU, 2014) [hereafter, "ITU Understanding Cybercrime"], at http://www.itu.int/en/ITU-D/Cybersecurity/Documents/cybercrime2014.pdf.

2. *See, e.g.,* Susan Brenner, "Thoughts, Witches and Crimes," CYB3RCRIM3: Observations on Technology, Law, and Lawlessness, (6 May 2009), at http://cyb3rcrim3.blogspot.com/2009/05/thoughts-witches-and-crimes.html (noting that "cybercrime is merely a method crime, *i.e.,* crime the commission of which is distinct due to the tool the perpetrator uses. […] cybercrime [can be addressed through…] traditional offenses that are revised, as necessary, to encompass the digital versions of these crimes").

3. From Shakespeare's "The Tempest," V.i, 186–189 (in which Miranda proclaims, "O wonder! / How many goodly creatures are there here! / How beauteous mankind is! O brave new world, / That has such people in't."), and used by Aldous Huxley in his 1931 novel by the same name (" 'O brave new world!' Miranda was proclaiming the possibility of loveliness, the possibility of transforming even the nightmare into something fine and noble. 'O brave new world!' It was a challenge, a command.").

4. Merriam-Webster Dictionary.

5. Black's Law Dictionary, 2d ed.

6. Maria Konnikova, "Virtual Reality Gets Real: The Promises—and Pitfalls—of the Emerging Technology," The Atlantic, (Oct. 2015), at http://www.theatlantic.com/magazine/archive/2015/10/virtual-reality-gets-real/403225/.

7. For a provocative fictional depiction thereof, and querying of what is "real," *see* Jennifer Haley, "The Nether" (Chicago: Northwestern Univ., 2015). For a review of the play, *see, e.g.,* Sadie Dingfelder, "'The Nether' at Woolly Mammoth Is a Creepy Puzzle of a Play," Washington Post, (7 Apr. 2016), at https://www.washingtonpost.com/express/wp/2016/04/07/the-nether-at-woolly-mammoth-is-a-creepy-puzzle-of-a-play/.

8. *See, e.g.,* WDR, *supra* § 1 A, note 10, which lays out a multitude of ways in which the internet and ICTs (mobile phones, computers and other technologies and tools) contribute to innovation, economic growth, economic and social inclusion and efficiencies, as well as attendant risks.

9. Ilia Kolochenko, "Cybercrime: The Price of Inequality," Forbes, (16 Dec. 2016), at http://www.forbes.com/sites/forbestechcouncil/2016/12/19/cybercrime-the-price-of-inequality/2/#1994040176db.

10. "Number of Internet Users Worldwide from 2005 to 2016 (in Millions)," Statista, at http://www.statista.com/statistics/273018/number-of-internet-users-worldwide/.

11. *See, e.g.,* Noah Rayman, "The World's Top 5 Cybercrime Hotspots," Time, (7 Aug. 2014), at http://time.com/3087768/the-worlds-5-cybercrime-hotspots/; Craig Silverman & Lawrence Alexander, "How Teens in the Balkans Are Duping Trump Supporters with Fake News," BuzzFeed News, (3 Nov. 2016), at https://www.buzzfeed.com/craigsilverman/how-macedonia-became-a-global-hub-for-pro-trump-misinfo?utm_term=.eiWv81lZY#.yrrb4qwgD.

12. "Norton Cybersecurity Insights Report 2016," Symantec, (2016), at https://us.norton.com/norton-cybersecurity-insights-report-global?inid=hho_norton.com_cybersecurityinsights_hero_seeglobalrpt.

13. *See also* "Cyberspace Policy Review," The White House of President Barack Obama, at https://obamawhitehouse.archives.gov/cyberreview/documents/.

14. *See also* "Leader of Hacking Ring Sentenced for Massive Identity Thefts from Payment Processor and US Retail Networks," US Dept. of Justice, (26 Mar. 2010), at https://www.justice.gov/sites/default/files/usao-nj/legacy/2014/09/02/dojgonzalez0326rel.pdf.

15. *United States v. Steven W. Chase,* 5:15-CR-00015-RLV-DCK-1 (W.D.N.C. 2016). To date, reports indicate that at least 137 cases have been brought around the United States following on from the FBI sting operation. *See, e.g.,* "The Playpen Cases: Frequently Asked Questions The Basics," Electronic Frontier Foundation, at https://www.eff.org/pages/playpen-cases-frequently-asked-questions#howmanycases. *See also* US Dept. of Justice, "Assistant Attorney General Leslie R. Caldwell Delivers Remarks Highlighting Cybercrime Enforcement at Center for Strategic and International Studies," Office of Public Affairs, (7 Dec. 2016), at https://www.justice.gov/opa/speech/assistant-attorney-general-leslie-r-caldwell-delivers-remarks-highlighting-cybercrime.

16. *See, e.g.,* Joseph Cox, "The FBI's 'Unprecedented' Hacking Campaign Targeted over a Thousand Computers," Motherboard, (5 Jan. 2016), at http://motherboard.vice.com/read/the-fbis-unprecedented-hacking-campaign-targeted-over-a-thousand-computers.

17. "Tor," Tor Project, at https://torproject.org/.

18. Duly named because it uses onion routing, a technique of layered encryption for anonymous communication over a computer network. *See, e.g.,* Joan Feigenbaum, Aaron Johnson & Paul Syverson, "A Model of Onion Routing with Provable Anonymity," Financial Cryptography & Data Security, (30 Aug. 2006), pp. 57–71, at http://www.cs.yale.edu/homes/jf/FJS.pdf.

19. Chris Baraniuk, "Tor Launches Anti-Censorship Messenger Service," BBC News (30 Oct. 2015), at http://www.bbc.com/news/technology-34677323.

20. *Ibid.*

21. *Ibid.*

22. Parliamentary Office of Science and Technology (POST), "The Darknet and Online Anonymity," UK Houses of Parliament, No.488 (9 Mar. 2015), at http://researchbriefings.parliament.uk/ResearchBriefing/Summary/POST-PN-488.

23. *See, e.g.,* "What is the Law?" Information Exchange Network for Mutual Assistance in Criminal Matters and Extradition (the "Network"), (2007), at https://www.oas.org/juridico/mla/en/can/en_can_mla_what.html.

24. For a discussion of the importance of public confidence in the banking systems, *see, e.g.,* Vincent Di Lorenzo, "Public Confidence and the Banking System: The Policy Basis for Continued Separation of Commercial and Investment Banking," 35 American Law Review, (1986), pp. 647–98, at http://www.stjohns.edu/sites/default/files/documents/law/dilorenzo-public_confidence_policy_basis.pdf. Public confidence stretches well-beyond banking and financial markets, with loss of confidence being attributed as one of the principle factors contributing to the fall of the Roman Empire. *See, e.g.,* Edward Gibbon, *The Decline and Fall of the Roman Empire,* (New York: Harcourt, Brace, 1960).

25. *See generally,* WDR *supra* § 1 A, note 10, at 221 *et seq.*

26. Thomas Weigend, "Information Society and Penal Law: General Report," *Revue internationale de droit pénal,* Vol. 84 (2013), p. 53.

27. Latin: *"horror vacui"*; a postulate of physics attributed to Aristotle.

28. An approximation of the notion of physics that the least energy state is preferable.

29. Francesca Spidalieri, *State of the States on Cybersecurity,* (Newport: Pell Center for International Relations, 2015), p. 3, at http://pellcenter.org/wp-content/uploads/2017/02/State-of-the-States-Report.pdf.

30. Brett Burns, "Level 85 Rogue: When Virtual Theft Merits Criminal Penalties," University of Missouri-Kansas City Law Review, Vol. 80 (2011), p. 845f.

31. US Government Accountability Office (GAO), *Public and Private Entities Face Challenges in Addressing Cyber Threats,* (Washington: GAO, 2007), p. 15, at http://www.gao.gov/new.items/d07705.pdf.

32. *See, e.g., ibid., 23;* CoE, *Convention on Cybercrime,* (23 Nov. 2001) ETS No. 185 [hereafter, "Budapest Convention"], Preamble, at https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185; Philippines: Cybercrime Prevention Act of 2012, No. 10175, Ch. II, Art. 4-A, at https://www.unodc.org/cld/en/legislation/phl/republic_act_no._10175_cybercrime_prevention_act_of_2012/chapter_ii/article_4-a/article_4-a.html.

33. David S. Wall, "Policing Cybercrimes: Situating the Public Police in Networks of Security within Cyberspace," Police Practice & Research, Vol. 8, Issue 2 (2007), pp. 183–205.

34. Brenner, *supra* note 2.

35. David S. Wall, "Cybercrime as a Conduit for Criminal Activity," in: A. Pattavina (ed.), *Information Technology and the Criminal Justice System,* (Beverly Hills, CA: Sage Publications, 2015), pp. 77–98.

36. Emilio Viano, "Cybercrime: A New Frontier in Criminology," International Annals of Criminology, Vol. 44 (2006), pp. 11–22.

37. Audrey Guinchard, "Cybercrime: The Transformation of Crime in the Digital Age," Information, Communication and Society, Vol. 11 (2008), pp. 1030–32.

38. *See, e.g.,* Stalking Resource Center, National Center for Victims of Crime, *Stalking Technology Outpaces State Laws,* Stalking Resource Center Newsletter, Vol. 3, No. 2 (2003), at https://victimsofcrime.org/docs/src/stalking-technology-outpaces-state-laws17A308005D0C.pdf?sfvrsn=2.

39. Emilio C. Viano, "§ II – Criminal Law. Special Part, Information Society and Penal Law, General Report," *Revue Internationale de Droit Pénal,* Vol. 84 (2013) 3–4, p. 339.

40. USC Title 18, § 1961. However, at least six types of fraud commonly charged in conjunction with USC Title 18, § 1030 are RICO predicate offenses, as are many serious offenses likely to underlie a cybercrime (trafficking in persons, interstate transportation of stolen property, murder for hire, etc.).

41. For more information on RICO, *see* Charles Doyle, "RICO: A Brief Sketch," US Congressional Research Service (CRS), No. 96-950 (18 May 2016), at https://fas.org/sgp/crs/misc/96-950.pdf.

42. Mark Gordon, "Ideas Shoot Bullets: How the RICO Act Became a Potent Weapon in the War Against Organized Crime," Concept, Vol. 26, (2002), at https://concept.journals.villanova.edu/article/view/312/275.

43. Weigend, *supra* note 26, at 51.

44. Full list of legislation in the United States concerning cyberbulling can be found under this address: http://cyberbullying.org/bullying-laws. For a broad analysis of cyberbullying law in the United States, *see* Megan Rehber & Susan W. Brenner, "'Kiddie Crime?' The Utility of Criminal Law in Controlling Cyberbullying," First Amendment Law Review, Vol. 8 (2009), pp. 73–78.

45. Weigend, *supra* note 26, at 53.

46. *Ibid.* at 52.

47. India: *State of Tamil Nadu vs. Suhas Katti* (CC No.4680/2004).

48. Allen Chein, "A Practical Look at Virtual Property," St. John's Law Review, Vol. 80 (2006), p. 1088f. *See also* Theodore J. Westbrook, "Owned: Finding a Place for Virtual World Property Rights," Michigan State Law Review (2006), p. 779ff.

49. In the RuneScape case, the Dutch Supreme Court decided that electronic goods are equal to tangible goods: "virtual goods are goods [under Dutch law], so this is theft"; Ben Kuchera, "Dutch Court Imposes Real-World Punishment for Virtual Theft," Ars Technica, (23 Oct. 2008), at https://arstechnica.com/gaming/2008/10/dutch-court-imposes-real-world-punishment-for-virtual-theft/.

50. The US Dept. of Justice prosecutes cases of identity theft and fraud under a variety of federal statutes. In 1998, Congress passed the Identity Theft and Assumption Deterrence Act, which created a new offense of identity theft and prohibiting "knowingly transfer[ring] or us[ing], without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law." USC Title 18, § 1028 - Fraud and Related Activity in Connection with Identification Documents, Authentication Features, and Information.

51. Jonathan Clough, "Data Theft? Cybercrime and the Increasing Criminalization of Access to Data," Criminal Law Forum, Vol. 22 (2011), pp. 145–70.

52. Alex Steel, "The True Identity of Australian Identity Theft Offences: A Measured Response or an Unjustified Status Offence?," University of New South Wales Law Journal, Vol. 33 (2010), pp. 503–531.

53. Soumyo D. Moitra, "Cybercrime: Towards an Assessment of its Nature and Impact, International Journal of Comparative & Applied Criminal Justice," Vol. 28, Issue 2 (2004), pp. 105–20.

54. Weigend, *supra* note 26, at 56.

55. Viano, *supra* note 39, at 341.

56. David S. Walls, "Cybercrime, Media and Insecurity: The Shaping of Public Perceptions of Cybercrime," International Review of Law, Computers and Technology, Special Issue: Crime and Criminal Justice, Vol. 22 (2008), pp. 45–63.

57. Leyla Bilge, Thorsten Strufe, Davide Balzarotti & Engin Kirda, "All Your Contacts Belong to Us: Automated Identity Theft Attacks on Social Networks," SBA Research, at http://www.cs.umd.edu/class/spring2017/cmsc396H/downloads/all-your-contacts.pdf.

58. Marco Gercke, "Internet-Related Identity Theft,"CoE Discussion Paper, (22 Nov. 2007), p. 4, at https://rm.coe.int/16802fa3a0.

59. Weigend, *supra* note 26, at 57.

60. Iain Moir & George R. S. Weir, "Identity Theft: A Study in Contact Centres," in: Hamid Jahankhani, Kenneth Revett & Dominic Palmer-Brown (eds.), *Global E-Security: Communications in Computer and Information Science*, Vol. 12 (Berlin: Springer, 2008), at http://www.cis.strath.ac.uk/cis/research/publications/papers/strath_cis_publication_2243.pdf.

61. A full list of identity fraud state regulations can be found at http://www.ncsl.org/issues-research/banking/identity-theft-state-statutes.aspx.

62. Walter A. Effross, "High-Tech Heroes, Virtual Villains, and Jacked-In Justice: Visions of Law and Lawyers in Cyberpunk Science Fiction," Buffalo Law Review, Vol. 46 (1997), p. 931.

63. For example, Venmo does not charge transaction fees for transferring funds between debit card or checking account, "Fees & Venmo," Venmo, at https://help.venmo.com/hc/en-us/articles/224361007-Fees-Venmo.

64. Moreover, the gap between technology and regulation is significant in FinTech. It will be important for regulators, while attempting to bridge this gap, to carefully support market development, while ensuring consumer security. John Villasenor, "Ensuring Cybersecurity in Fintech: Key Trends and Solutions," Forbes, (25 Aug. 2016), at http://www.forbes.com/sites/johnvillasenor/2016/08/25/ensuring-cybersecurity-in-fintech-key-trends-and-solutions/#13edc74be1fa.

65. For an overview of data partitioning, *see* Microsoft Website, at https://docs.microsoft.com/en-us/azure/best-practices-data-partitioning.

66. Jamie Smith, "There Is More to Blockchain than Moving Money. It Has the Potential to Transform Our Lives—Here's How," World Economic Forum, (9 Nov. 2016), at https://www.weforum.org/agenda/2016/11/there-is-more-to-blockchain-than-moving-money.

67. *See, e.g.*, Kariappa Bheemaiah, "Block Chain 2.0: The Renaissance of Money," Wired, (Jan. 2015), at https://www.wired.com/insights/2015/01/block-chain-2-0/.

68. "How Blockchains Could Change the World," McKinsey & Company, (May 2016), at http://www.mckinsey.com/industries/high-tech/our-insights/how-blockchains-could-change-the-world.

69. Mary-Ann Russon, "Quantum Cryptography Breakthrough: 'Unbreakable Security' Possible Using Pulse Laser Seeding," International Business Times (7 Apr. 2016), at http://www.ibtimes.co.uk/quantum-cryptography-breakthrough-unbreakable-security-possible-using-pulse-laser-seeding-1553721.

70. *Ibid.*

71. WDR, *supra* § 1 A, note 10, at 223. For an interesting perspective on the interrelation of analog and digital, *see* Peter Kinget, "The World Is Analog," Circuit Cellar, No. 292 (Nov. 2014), at http://www.ee.columbia.edu/~kinget/WhyAnalog/circuitcellar_The_World_Is_Analog_201410.pdf.

72. WDR, *supra* § 1 A, note 10, at 223.

73. *Association Internationale de Droit Pénal* (AIDP/IAPL), 19th International Congress of Penal Law, (Aug. 2014), § 1.A.1, (noting, in relevant part, that "ICT and cyberspace have created specific interests which must be respected and protected, for example, privacy, confidentiality, integrity and availability of ICT systems as well as the integrity of personal identities in cyberspace").

74. Xavier Amadei, "Standards of Liability for Internet Service Providers: A Comparative Study of France and the United States with a Specific Focus on Copyright, Defamation, and Illicit Content," Cornell International Law Journal, Vol. 35 (1) (2001), at http://scholarship.law.cornell.edu/cilj/?utm_source=scholarship.law.cornell.edu%2Fcilj%2Fvol35%2Fiss1%2F4&utm_medium=PDF&utm_campaign=PDFCoverPages.

75. Ronald Noble, Former INTERPOL Secretary General, at https://cdn.press.kaspersky.com/files/2013/06/Kaspersky-Lab-Transparency-Principles_Q3_2015_final.pdf.

76. Internet Security Alliance, "Cross Cutting Issue #2: How Can We Create Public Private Partnerships that Extended to Action Plans that Work?," The White House of Barack Obama, at https://obamawhitehouse.archives.gov/files/documents/cyber/ISA%20-%20Hathaway%20public%20private%20partnerships.pdf.

77. Executive Order—Promoting Private Sector Cybersecurity Information Sharing, (13 Feb. 2015). *See also* "Executive Order -- Promoting Private Sector Cybersecurity Information Sharing," The White House of President Barack Obama, Press Release, (13 Feb. 2015), at https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari; Gregory Korte, "Obama Signs Two Executive Orders on Cybersecurity," USA Today, (9 Feb. 2016), at http://www.usatoday.com/story/news/politics/2016/02/09/obama-signs-two-executive-orders-cybersecurity/80037452/.

78. Pres. Barack Obama, "Remarks by the President on Securing Our Nation's Cyber Infrastructure," The White House Office of the Press Secretary, The White House of President Barack Obama, (29 May 2009), at https://obamawhitehouse.archives.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure.

79. On 18 December 2015, the European Commission launched a public consultation, accompanied by a policy roadmap, to seek stakeholders' views on the areas of work of a future public-private partnership, as well as on potential additional policy measures—in areas such as certification, standardization and labeling—that could benefit the European cybersecurity industry. To strengthen EU's cybersecurity industry, the European Commission will establish a contractual Public-Private Partnership (cPPP) on cybersecurity, as envisaged in the Digital Single Market Strategy. The aim of the PPP is to stimulate the European cybersecurity industry by: bringing together industrial and public resources to improve Europe's industrial policy on cybersecurity, focusing on innovation and following a jointly-agreed strategic research and innovation roadmap; helping build trust among Member States and industrial actors by fostering bottom-up cooperation on research and innovation; helping stimulate cybersecurity industry by aligning the demand and supply for cybersecurity products and services, and allowing the industry to efficiently elicit future requirements from end-users; leveraging funding from Horizon2020 and maximizing the impact of available industry funds through better coordination and better focus on a few technical priorities; and providing visibility to European R&I excellence in cyber security and digital privacy. *See also* Commissioner, "Digital Single Market," European Commission, at http://ec.europa.eu/priorities/digital-single-market/.

80. Warwick Ashford, "Co-Operation Driving Progress in Fighting Cybercrime, Say Law Enforcers," Computer Weekly, (5 Jun. 2015), at http://www.computerweekly.com/news/4500247603/Co-operation-driving-progress-in-fighting-cyber-crime-say-law-enforcers.

81. *See also* Actual Order Compelling Apple, Inc. to Assist Agents in Search of iPhone,"Cybersecuritylaw, at http://blog.cybersecuritylaw.us/2016/02/23/actual-order-compelling-apple-inc-to-assist-agents-in-search-of-iphone/.

82. *See, e.g.,* Saeed Ahmed, "Who Were Syed Rizwan Farook and Tashfeen Malik?," CNN, (4 Dec. 2015), at http://www.cnn.com/2015/12/03/us/syed-farook-tashfeen-malik-mass-shooting-profile/index.html.

83. *See* Julia Edwards, "FBI Paid More Than $1.3 Million to Break into San Bernardino iPhone," Reuters, (22 Apr. 2016), at http://www.reuters.com/article/us-apple-encryption-fbi-idUSKCN0XI2IB.

84. Kim Zetter, "The Feds' Battle with Apple Isn't Over—It Just Moved to New York," Wired, (8 Apr. 2016), at https://www.wired.com/2016/04/feds-battle-apple-isnt-just-moved-ny/.

85. Nathaniel Mott, Take That, "FBI: Apple Goes All in on Encryption," The Guardian, (15 Jun. 2016), at https://www.theguardian.com/technology/2016/jun/15/apple-fbi-file-encryption-wwdc.

86. Cade Metz, "Forget Apple vs. the FBI: WhatsApp Just Switched on Encryption for a Billion People," Wired, (5 Apr. 2016), at http://www.wired.com/2016/04/forget-apple-vs-fbi-whatsapp-just-switched-encryption-billion-people/.

87. *See, e.g.,* Ivana Kottasova and Samuel Burke, "UK Government Wants Access to WhatsApp Messages," CNN Tech, (27 Mar. 2017), at http://money.cnn.com/2017/03/27/technology/whatsapp-encryption-london-attack/index.html.

88. *See, e.g.,* Amber Rudd, Home Secretary, "Social Media Firms Must Join the War on Terror," Telegraph, (25 Mar. 2017) ("We need the help of social media companies, the Googles, the Twitters, the Facebooks of this world. And the smaller ones, too: platforms such as Telegram, WordPress and Justpaste.it. We need them to take a more proactive and leading role in tackling the terrorist abuse of their platforms. We need them to develop further technology solutions. We need them to set up an industry-wide forum to address the global threat."), at http://www.telegraph.co.uk/news/2017/03/25/social-media-firms-must-join-war-terror/; UK Home Secretary, "We need the Help of Social Media Companies," UK Home Office News Team, (26 Mar. 2017), at https://homeofficemedia.blog.gov.uk/2017/03/26/home-secretary-we-need-the-help-of-social-media-companies/.

89. *See, e.g.,* Peter Walker and Heather Stewart, "No 10 Repeats Rudd's Call for Authorities to Access Encrypted Messages," Guardian, (27 Mar. 2017), at https://www.theguardian.com/politics/2017/mar/27/downing-street-amber-rudd-authorities-access-encrypted-messages-whatsapp-terrorism.

90. Thomas Boué, "Closing the Gaps in EU Cyber Security," Computer Weekly, (Jun. 2015), at http://www.computerweekly.com/opinion/Closing-the-gaps-in-EU-cyber-security.

91. "Number of Internet Users Worldwide from 2000 to 2015 (in Millions)," Statista, at http://www.statista.com/statistics/273018/number-of-internet-users-worldwide/.

92. *See, e.g.,* Tim Bajarin, "The Next Big Thing for Tech: The Internet of Everything," Time, (13 Jan. 2014), at http://time.com/539/the-next-big-thing-for-tech-the-internet-of-everything/.

93. *See* WDR § 1 A, *supra* note 10.

Referenced in: § C. Challenges to Fighting Cybercrime

1. ITU Understanding Cybercrime, *supra* § 1 B, note 1.
2. *See, e.g.,* US Access Board, § 508 - Standards for Electronic and Information Technology, Final Rule, (21 Dec. 2000).
3. *Ibid.,* at 75.
4. *See, e.g.,* Kristin Finklea & Catherine A. Theohary, *Cybercrime: Conceptual Issues for Congress and US Law Enforcement,* US Congressional Research Service (CRS), (2015), p. 16 (provides that "For instance, identity theft (18 USC § 1028(a)(7)) is a crime whether it is committed solely in the real world or carried out via cyber means. The statute does not distinguish between the means by which the crime is carried out"), at https://www.fas.org/sgp/crs/misc/R42547.pdf.
5. For example, "wire transfer" and "stalking".
6. Such as "place" and "document".
7. UN Office of Drugs and Crime (UNODC), *Comprehensive Study on Cybercrime (Draft)* [hereafter, "UNODC Cybercrime Study"], (New York: United Nations, 2013), p. 58, at https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.
8. One famous conception of just such a scenario is in the 1968 cult-classic film *2001: A Space Odyssey,* where the spacecraft's computer, HAL—short for "heuristically-programmed algorithmic computer"—"decides" to terminate the human team members when it becomes apparent that the humans, who are unaware of the mission's real purpose, may jeopardize that purpose. Stanley Kubrick, dir. *2001: A Space Odyssey.* Writ. Arthur C. Clarke & Stanley Kubrick. Metro Goldwyn-Mayer (MGM), 1968. Film.
9. *United States v. Liberty Reserve et al.,* 13 Cr. 368, UNODC Cybercrime Repository, at https://www.unodc.org/cld/case-law-doc/cybercrimecrimetype/usa/2014/us_v_liberty_reserve_et_al..html?&tmpl=cyb; *Indictment & Supporting Documents: United States v. Liberty Reserve et al.,* (S.D.N.Y. 2013), at http://www.justice.gov/usao/nys/pressreleases/May13/LibertyReserveetalDocuments.php; Emily Flitter, "US Accuses Currency Exchange of Laundering $6 Billion," Reuters, (29 May 2013), at http://www.reuters.com/article/2013/05/29/net-us-cybercrime-libertyreserve-charges-idUSBRE94R0KQ20130529.
10. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act), No. 107–56, 115 Stat. 272 (2001) [hereafter, "USA PATRIOT Act"].
11. *See infra* § 2 B.
12. Technological neutrality refers to the drafting of laws that are technologically agnostic, that is, laws that do not specifically refer to any particular technology. Doing so not only assures that online and offline conduct is treated equally, but also assures that the law is not so easily outdated by technological progress. This strategy, refraining from naming any device or software or using a nonexclusive list, punishes a criminal conduct as long as the effect is felt. Moreover, not naming a specific technology allows laws to stay relevant even after new device or criminal methodology is developed. *See* "Technology Neutrality in Internet, Telecoms and Data Protection Regulation," Hogan Lovells Global Media and Communications Quarterly, (2014), at http://www.hoganlovells.com/files/Uploads/Documents/8%20Technology%20neutrality%20in%20Internet.pdf.
13. *See, e.g.,* WDR, *supra* § 1 A, note 10, at 222, noting "Public safety and security in the analog world is a public good, ensured by governments. In the cyberworld, governments also have an obligation […] to ensure the protection of data, communications, and critical infrastructure." *See also* ITU Understanding Cybercrime, *supra* § 1 B, note 1, at 82–84.
14. Supreme Court of Korea, Decision 2014 No. 8838 (13 Nov. 2014), at http://www.law.go.kr/precInfoP.do?mode=0&precSeq=176320 (*in Korean*). *See also* Seoul Central District Court, Decision 2014 No.323 (26 Jun. 2014), at http://www.law.go.kr/precInfoP.do?evtNo=2014%eb%85%b8323 (*in Korean*); Seoul Central District Court, Decision No.4451, 4488 (Consolidation) (15 Jan. 2014), at http://mobile.law.go.kr/LSWM/mobile/precScInfo.do;jsessionid=plrVTdB8eoKZ1bXXaJl0wla9S2E44BfcfQGizaMGLE3jt081q9o0TtHznXov6JFN.de_kl_a6_servlet_PRM?precSeq=176605&precScNm=%ED%8C%90%EB%A1%80&searchKeyword=&pageIndex=127&name=precSc (*in Korean*).
15. Korea: Game Industry Promotion Act, at http://elaw.klri.re.kr/eng_mobile/viewer.do?hseq=28802&type=sogan&key=8 (*in English*).
16. *Ibid.,* Art. 18-3(c).
17. *Ibid.*
18. Rohini Tendulkar, *Securities Markets and Systemic Risk: Joint Staff Working Paper of the IOSCO Research Department and World Federation of Exchanges,* IOSCO Research Department, at pp. 4 & 22, at http://www.iosco.org/research/pdf/swp/Cyber-Crime-Securities-Markets-and-Systemic-Risk.pdf.
19. *Ibid.*
20. *Ibid.* at 4.
21. *United States v. Albert Gonzalez,* D. Mass. (No. 10223 & No. 10382).
22. Kim Zetter, "TJX Hacker Gets 20 Years in Prison," Wired, (25 Mar. 2010), at https://www.wired.com/2010/03/tjx-sentencing/.
23. Edecio Martinez, "Albert Gonzalez, 'SoupNazi' Credit Card Hacker Gets 20 Years," CBS News, (26 Mar. 2010), at http://www.cbsnews.com/news/albert-gonzalez-soupnazi-credit-card-hacker-gets-20-years/; Kim Zetter, "In Surprise Appeal, TJX Hacker Claims US Authorized His Crimes," Wired, (7 Jul. 2011), at http://www.wired.com/2011/04/gonzalez-plea-withdrawal/.
24. Do Punishments Fit the Cybercrime?," 2010, InfoSecurity Magazine, (25 Aug. 2010), at https://www.infosecurity-magazine.com/magazine-features/do-punishments-fit-the-cybercrime/.
25. L. Thomas Winfree, Jr., G. Larry Mays & Leanne Fiftal Alarid *Introduction to Criminal Justice* (New York: Wolters Kluwer, 2015

26. *See infra* § 2 C.

27. The *ultima ratio* principle emphasizes the repressive nature of the criminal justice system and classifies it as the last resort of the legislator. *See, e.g.,* Sakari Melander, "Ultima Ratio in European Criminal Law," Oñate Socio-Legal Series, Vol. 3 (2013); Rudolf Wendt, "The Principle of Ultima Ratio and/or the Principle of Proportionality," Oñate Socio-Legal Series, Vol. 3 (2013); Markus D. Dubber, "Ultima Ratio as Caveat Dominus: Legal Principles, Police Maxims and the Critical Analysis of Law," SSRN (5 Jul. 2013), at http://ssrn.com/abstract=2289479.

28. Kathleen Fuller, "ICANN: The Debate Over Governing the Internet," Duke Law & Technology Review, Vol. 2 (2001); Mary B. Kibble, "Fear Mongering, Filters, the Internet and the First Amendment: Why Congress Should Not Pass Legislation Similar to the Deleting Online Predators Act," Roger Williams University Law Review, Vol. 13 (2007), p. 497.

29. Anita Bernstein, "Social Networks and the Law: Real Remedies for Virtual Injuries," North Carolina Law Review, Vol. 90 (Jun. 2012), p. 1457; "New Bill Gives Turkish Government Power to Shut Down Websites in Four Hours," BBC Monitoring Europe, (23 Mar. 2015); Nicholas Cecil, "MP Demands Law to Force Internet Providers to Remove Gang Videos," Evening Standard, (6 Nov. 2011), at http://www.standard.co.uk/news/mp-demands-law-to-force-internet-providers-to-remove-gang-videos-6365780.html; Wayne McCormack, "US Judicial Independence: Victim in the 'War on Terror,'" Washington & Lee Law Review, Vol. 71 (2014), p. 305.

30. Mary M. Cheh, "Constitutional Limits on Using Civil Remedies To Achieve Criminal Law Objectives: Understanding and Transcending the Criminal-Civil Law Distinction," Hastings Law Journal, Vol. 42 (1991), p. 1325; Julie Adler, "The Public's Burden in a Digital Age: Pressures on Intermediaries & the Privatization of Internet Censorship," Journal of Law & Policy, Vol. 20 (2011), p. 231; James R. Marsh, "Predators, Porn and the Law: America's Children in the Internet Era: A Federal Civil Remedy for Child Pornography Victims," Syracuse Law Review, Vol. 61 (2015), p. 459; Joseph Salvador, "Dismantling the Internet Mafia: RICO's Applicability to Cyber Crime," Rutgers Computer & Technology Law Journal, Vol. 41 (2015), p. 268. Microsoft has used civil actions to attack botnets. *See* Official Microsoft Blog, "Botnets," Microsoft, at https://blogs.microsoft.com/blog/tag/botnets/#sm.000013htf1t8ngf0zuycn3473chdh.

31. *See, e.g.,* WDR, *supra* § 1 A, note 10, at 223; *see also* Bauer, Johannes & Bill Dutton, *Addressing the Cybersecurity Paradox: Economic and Cultural Challenges to an Open and Global Internet,* Background Paper for the World Development Report 2016, (Washington: World Bank, 2016).

32. Emilio Viano, "Balancing Liberty and Security Fighting Cybercrime: Challenges for the Networked Society," in: Stefano Manacorda (ed.), *Cybercriminality: Finding a Balance between Freedom and Security* (Milano: ISPAC Editora, 2012), pp. 33–64.

33. Russell G. Smith, Ray Chak-Chung Cheung & Laurie Yiu-Chung Lau, *Cybercrime Risks and Responses: Eastern and Western Perspectives,* (London: Palgrave MacMillan, 2015), p. 47.

34. David Kushner, "The Real Story of Stuxnet: How Kaspersky Lab Tracked Down the Malware that Stymied Iran's Nuclear-Fuel Enrichment Program," IEEE Spectrum, (26 Feb. 2013), at http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet.

35. *Ibid.*

36. Michael S. Schmidt, "Cybersecurity Bill Is Blocked in Senate by G.O.P. Filibuster," New York Times, (2 Aug. 2012), at: http://www.nytimes.com/2012/08/03/us/politics/cybersecurity-bill-blocked-by-gop-filibuster.html?_r=0.

37. Fuller, *supra* note 28.

38. *See* AIDP/IAPL, *supra* § 1 B, note 73.

39. Mott, *supra* § 1 B, note 85.

40. "Ransomware Cyber-attack Threat Escalating—Europe," BBC News, (14 May 2017), at http://www.bbc.com/news/technology-39913630.

41. "WannaCry: What Is Ransomware and How to Avoid It," Al Jazeera, (16 May 2017), at http://www.aljazeera.com/news/2017/05/ransomware-avoid-170513041345145.html; Victoria Woollaston, "Wanna Decryptor Ransomware Appears to be Spawning and This Time It May Not Have a Kill Switch," Wired, (16 May 2017), at http://www.wired.co.uk/article/wanna-decryptor-ransomware. Typically, hackers rely on tricking users to click on attachments harboring attack code, and email is the still the preferred attack tool. *Ibid. See also 2017 Internet Security Threat Report, Symantec,* at https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf.

42. Early linguistic analysis by Flashpoint indicated a Chinese connection: of the 28 languages in which the ransom notice was written, only the Chinese (both Simplified and Traditional) and English versions were written by humans instead of machine-translated, and only the Chinese notice appears to have been written by a fluent speaker; the other messages, including the Korean message, were apparently translated from the English note using Google Translate. *See* Jon Condra, John Costello & Sherman Chu, "Linguistic Analysis of WannaCry Ransomware Messages Suggests Chinese-Speaking," Flashpoint, (25 May 2017), at https://www.flashpoint-intel.com/blog/linguistic-analysis-wannacry-ransomware/. However, more in-depth and nuanced forensic analyses points to criminals from North Korea; that said, no connection to the North Korea state itself had been demonstrated. The cybersecurity service firm Symantec showed "strong links" to Lazarus group, a hacking group based in Pyongyang and closely associated with the North Korean government. *See* Symantec Security Response, "WannaCry: Ransomware Attacks Show Strong Links to Lazarus Group," Symantec Official Blog, (22 May 2017), at https://www.symantec.com/connect/blogs/wannacry-ransomware-attacks-show-strong-links-lazarus-group. That analysis has been since supported by an investigation led by Britain's National Cyber Security Centre (NCSC) and supported by the US-CERT. *See, e.g.,* Gordon Corera, "NHS Cyber-Attack Was 'Launched from North Korea,'" BBC News, (16 Jun. 2017), at http://www.bbc.com/news/technology-40297493. Lazarus group has been blamed for the 2014 cyberattack on Sony and the theft of US$81m from Bangladesh's central bank. "More Evidence for WannaCry 'Link' to North Korean Hackers," BBC News, (23 May 2017), at http://www.bbc.com/news/technology-40010996. As already noted, such matters are beyond the scope of the Toolkit. *See supra* § 1 A.

43. MalwareTech, "How to Accidentally Stop a Global Cyber Attacks," MalwareTech Blog, (13 May 2017), at https://www.malwaretech.com/2017/05/how-to-accidentally-stop-a-global-cyber-attacks.html. The researcher noted that the malware attempted to contact a specific web address each time it infected a new system; the address not being registered, he did so himself, allowing him to see where computers were being affected and unexpectedly triggering a part of the code that told the ransomware to stop spreading. *Ibid.*

44. Speaking to the BBC, MalwareTech said, "There's a lot of money in this, there is no reason for them to stop. It's not much effort for them to change the code and start over." Chris Foxx, "Global Cyber-attack: Security Blogger Halts Ransomware 'by Accident'," BBC News, (14 May 2017), at http://www.bbc.com/news/technology-39907049.

45. Dave Lee, "Global Cyber-Attack: How Roots Can be Traced to the US," BBC News, (13 May 2017), at http://www.bbc.com/news/technology-39905509. The NSA has neither confirmed nor denied as much. It is not known who conducted the attacks. It has been suggested that the NSA may have created the tool. Id.; Bill Chappell, "WannaCry Ransomware: Microsoft Calls Out NSA For 'Stockpiling' Vulnerabilities," NPR, (15 May 2017), at http://www.npr.org/sections/thetwo-way/2017/05/15/528439968/wannacry-ransomware-microsoft-calls-out-nsa-for-stockpiling-vulnerabilities; Thomas Fox-Brewster, "An NSA Cyber Weapon Might Be Behind A Massive Global Ransomware Outbreak," Forbes, (12 May 2017), at http://www.npr.org/sections/thetwo-way/2017/05/15/528439968/wannacry-ransomware-microsoft-calls-out-nsa-for-stockpiling-vulnerabilities.

46. Andy Greenberg, "Major Leak Suggests NSA Was Deep in Middle East Banking System," Wired, (14 Apr. 2017), at https://www.wired.com/2017/04/major-leak-suggests-nsa-deep-middle-east-banking-system/.

47. Bill Chappell, "WannaCry Ransomware: What We Know Monday," NPR, (15 May 2017), at http://www.npr.org/sections/thetwo-way/2017/05/15/528451534/wannacry-ransomware-what-we-know-monday.

48. "WannaCry: Are You Safe?," Kaspersky Labs, (13 May 2017), at https://blog.kaspersky.com/wannacry-ransomware/16518/; "Kaspersky Lab's Notice to Customers about the Shadow Brokers' Publication from April 14," Kaspersky Labs, (14 Apr. 2017), at https://support.kaspersky.com/shadowbrokers.

49. US policy had been understood to be one of disclosing identified vulnerabilities to vendors and others so that they can be patched. *See* Kim Zetter, "Obama: NSA Must Reveal Bugs Like Heartbleed, Unless They Help the NSA," Wired, (15 Apr. 2014), at https://www.wired.com/2014/04/obama-zero-day/. Such being the case, it is not clear why the vulnerabilities identified had not been released. *See* Brad Smith, "The Need for Urgent Collective Action to Keep People Safe Online: Lessons from Last Week's Cyberattack," Official Microsoft Blog, (14 May 2017), at https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/#oHaqtHbEYodLhwLl.99. *See also* Matt Day, "Microsoft Criticizes Government Creation of Hacking Tools Used in Global Cyberattack," Seattle Times, (14 May 2017), at http://www.seattletimes.com/business/microsoft/microsoft-criticizes-government-creation-of-hacking-tools-used-in-global-cyberattack/.

50. "Next Cyber-attack Could Be Imminent, Warn Experts," BBC News (14 May 2017), at http://www.strategic-culture.org/news/2017/05/14/international-cyber-attack-roots-traced-us-national-security-agency.html; Victoria Woollaston, "Wanna Decryptor Ransomware Appears to Be Spawning and This Time It May Not Have a Kill Switch," Wired, (16 May 2017), at http://www.wired.co.uk/article/wanna-decryptor-ransomware.

51. In March 2017, Microsoft released a patch for the vulnerability in question. Microsoft, Security Bulletin MS17-010, (14 Mar. 2017), at https://technet.microsoft.com/en-us/library/security/ms17-010.aspx. Following the attacks in May, Microsoft released a separate patch for users of older and unsupported operating systems, such as Windows XP.

52. MSRC Team, "Customer Guidance for WannaCrypt Attacks," Microsoft Official Blog, (12 May 2017), at https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/.

53. *2017 Data Breach Investigations Report,* 10th ed., Verizon, (27 Apr. 2017), at http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/.

54. *See, e.g.,* Dave Lee, "Global Cyber-Attack: How Roots Can Be Traced to the US," BBC News, (13 May 2017), at http://www.bbc.com/news/technology-39905509.

55. *Cybercrime Knows No Borders,* InfoSecurity Magazine, (19 May 2011), at http://www.infosecurity-magazine.com/magazine-features/cybercrime-knows-no-borders/.

56. WDR, *supra* § 1 A, note 10, at 222. While such actions "blur[ ] the lines between acts of cybercrime and cyberwar or cyberterrorism," it is nonetheless the responsibility of the government to assure public safety and security in cyberspace. *Ibid.* at 223.

57. The first free, widely used end-to-end encrypted messaging software was PGP ("Pretty Good Privacy"), coded by Phil Zimmermann and released in 1991. Andy Greenberg, "Hacker Lexicon: What Is End-to-End Encryption?," Wired, (25 Nov. 2014), at https://www.wired.com/2014/11/hacker-lexicon-end-to-end-encryption/.

58. Greenberg, *ibid.*

59. *Ibid.*

60. Information theory can be used to render a cryptosystem information-theoretically secure, and therefore cryptanalytically unbreakable, even when the adversary has unlimited computing power. Ueli Maurer, "Information-Theoretically Secure Secret-Key Agreement by NOT Authenticated Public Discussion," in: EUROCRYPT'97 Proceedings of the 16th annual international conference on Theory and application of cryptographic techniques, (1997), pp. 209–25, at ftp://ftp.inf.ethz.ch/pub/crypto/publications/Maurer97.pdf.

61. Greenberg, *supra* note 57.

62. PFS-perfect forward secrecy is a technique used, for instance, by TextSecure, an SMS application for Android, and the software integrated by WhatsApp into its messaging services. *See, e.g.,* Dan Goodin, "WhatsApp Brings Strong End-to-end Frypto to the Masses," Quora, (18 Nov. 2014), at https://www.quora.com/How-secure-is-WhatsApps-new-end-to-end-encryption.

63. For a discussion of the mathematics behind cracking computer cyphers, *see, e.g.,* "The Math Behind Estimations to Break a 2048-bit Certificate," DigiCert, at https://www.digicert.com/TimeTravel/math.htm.

64. "256-bit AES key" means that every 256-bit number is a valid key or modulus. Having superseded DES (Data Encryption Standard), AES (Advanced Encryption Standard) is a symmetric encryption algorithm (specifically, a block cypher) in use worldwide, which is defined over keys of 128, 192 and 256 bits. Symmetric algorithms are designed to be as simple and quick as possible (for cryptography), and retain a high level of security. *See, e.g.,* "Why Do You Need a 4096-bit DSA Key When AES Is Only 256-Bits?," Information Security Stack Exchange, at http://security.stackexchange.com/questions/59190/why-do-you-need-a-4096-bit-dsa-key-when-aes-is-only-256-bits; "What Does 'Key with Length of X Bits' Mean?," Information Security Stack Exchange, at http://security.stackexchange.com/questions/8912/what-does-key-with-length-of-x-bits-mean.

65. "Why Do You Need a 4096-bit DSA Key When AES Is Only 256-Bits?," *ibid.*

66. Mary-Ann Russon, "Quantum Cryptography Breakthrough: 'Unbreakable Security' Possible Using Pulse Laser Seeding," International Business Times, (7 Apr. 2016), at http://www.ibtimes.co.uk/quantum-cryptography-breakthrough-unbreakable-security-possible-using-pulse-laser-seeding-1553721. China has made particular advances in the development of such technology; for the implications of implications of such advances, *see* Andreas Illmer, "China Set to Launch an 'Unhackable' Internet Communication," BBC News, (25 July 2017), at http://www.bbc.com/news/world-asia-40565722.

67. Greenberg, *supra* note 57.

68. *See also* Nandagopal Rajan, "WhatsApp Is Not Breaking Indian Laws with 256-Bit Encryption, for Now," Indian Express, (12 Apr. 2016), at http://indianexpress.com/article/technology/social/whatsapp-end-to-end-encryption-not-illegal-in-india/.

69. Russon, *supra* note 66.

70. Brendan J. Sweeney, Global Competition: Searching for a Rational Basis for Global Competition Rules, Sydney Law Review, Vol. 30 (2008), p. 209.

71. Budapest Convention, *supra* § 1 B, note 32.

72. EU Council Framework Decision 2005/222/JHA (24 Feb. 2005) on Attacks against Information Systems, at http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32005F0222.

73. EU Council Framework Decision 2004/68/JHA (22 Dec. 2003) on combating the sexual exploitation of children and child pornography. The Framework Decision was replaced by Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography. *See* OJ 2011 L 335 (17 Dec. 2011), pp. 1–17.

74. Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC [2006] OJ L105/54 ("Data Retention Directive").

75. *European Commission v. Hungary,* [hereafter, *"Commission v. Hungary"*], Case number C-286/12, [CJEU] (8 Apr. 2014), at http://curia.europa.eu/juris/documents.jsf?num=C-293/12; EUR-Lex, Official Journal of the European Union, (8 Apr. 2014).

76. Richard W. Downing, "Shoring Up the Weakest Link: What Lawmakers Around the World Need to Consider in Developing Comprehensive Laws to Combat Cybercrime," Columbia Journal of Transnational Law, Vol. 43 (2005), p. 705; Erin I. Kunze, "Sex Trafficking Via the Internet: How International Agreements Address the Problem and Fail to Go Far Enough," Journal on Telecommunications & High Technology Law, Vol. 10 (2010), p. 241; Miriam F. Miquelon-Weismann, "The Convention on Cybercrime: A Harmonized Implementation of International Penal Law: What Prospects for Procedural Due Process," John Marshall Journal Computer & Informational Law, Vol. 23 (2005), p. 329; Deborah Griffith Keeling & Michael M. Losavio, "A Comparative Review of Cybercrime Law and Digital Forensics in Russia, the United States and under the Convention on Cybercrime of the Council of Europe," Northern Kentucky University Law Review, Vol. 39 (2012), p. 267.

77. Viano, *supra* § 1 B, note 39, at 342–44.

78. *Ibid.,* at 347–53.

79. *Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse,* CoE, (25 Oct. 2007) CETS No. 201 [hereafter, "Lanzarote Convention"], at http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=201&CM=&DF=&CL=ENG.

80. *See, e.g., Additional Protocol to the Council of Europe Convention on Cybercrime Concerning the Criminalization of Acts of a Racist and Xenophobic Nature Committed through Computer Systems,* CoE (2003), at http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm.

81. International Narcotics Control Board, "Globalization and New Technologies: Challenges to Drug Law Enforcement in the Twenty-First Century," (2001), at https://www.incb.org/documents/Publications/AnnualReports/AR2001/AR_01_Chapter_I.pdf; ITU Understanding Cybercrime, *supra* § 1 B, note 1, pp. 30–40; Stefan Frederick Fafinski, "Computer Use and Misuse: The Constellation of Control," Ph.D. Dissertation, University of Leeds, School of Law, (2008), pp. 273–81.

82. *See, e.g.,* "Europol Supports Huge International Operation to Tackle Organised Crime," Europol, at https://www.europol.europa.eu/content/europol-supports-huge-international-operation-tackle-organised-crime.

83. Eric Neumayer, "Qualified Ratification: Explaining Reservations to International Human Rights Treaties," Journal of Legal Studies, Vol. 36 (2007), p. 397.

84. Budapest Convention, *supra* § 1 B, note 32, at Art. 42.

85. ITU Understanding Cybercrime, *supra* § 1 B, note 1, at 77–78.

86. For example, according to "Cybercrime knows no borders" featured by InfoSecurity Magazine in 2011, Invincea founder Anup Ghosh notes that "Law enforcement agencies don't have jurisdiction to prosecute outside their borders, so they need bilateral or multi-lateral agreements to bring criminals to justice. But often it is really just sharing information with foreign law enforcement agencies and hoping they will do something about it." For additional information: *Ibid.*

87. *See infra* § 2 E.

88. Anthony J. Colangelo, "A Unified Approach to Extraterritoriality," Virginia Law Review, Vol. 97 (2011), p. 1019.

89. *United States v. Aleksandr Andreevich Panin, a/k/a Harderman, a/k/a Gribodemon, and Hamza Bendelladj, a/k/a Bx1,* (26 Jun. 2013) N.D. Ga., No. 1:11-cr-00557-AT-AJB Document 35.

90. Christopher Budd, "Why the SpyEye Conviction is a Big Deal," Trend Micro, (3 Feb. 2014), at http://blog.trendmicro.com/spyeye-conviction-big-deal/.

91. "SpyEye Botnet Kit Developer Sentenced to Long Jail Term," PC World, (20 Apr. 2016), at http://www.pcworld.com/article/3059557/spyeye-botnet-kit-developer-sentenced-to-long-jail-term.html.

92. US Attorney's Office, N.D. Ga., "Cyber Criminal Pleads Guilty to Developing and Distributing Notorious SpyEye Malware," (28 Jan. 2014), at https://archives.fbi.gov/archives/atlanta/press-releases/2014/cyber-criminal-pleads-guilty-to-developing-and-distributing-notorious-spyeye-malware/.

93. "Two Major International Hackers Who Developed the 'SpyEye' Malware Get Over 24 Years Combined in Federal Prison," US Dept. of Justice, (26 Apr. 2016), at https://www.justice.gov/usao-ndga/pr/two-major-international-hackers-who-developed-spyeye-malware-get-over-24-years-combined.

94. *Ibid.*

95. *Ibid. See also* US Attorney's Office, *supra* note 92.

96. UNODC Cybercrime Study, *supra* § 1 C, note 7, at 108.

97. *See infra* § 5 A.

98. Fernando Molina, "A Comparison between Continental European and Anglo-American Approaches to Overcriminalization and Some Remarks on How to Deal with It," New Criminal Law Review, Vol. 14 (2011), p. 123; Kimberly Kessler Ferzan, "Prevention, Wrongdoing, and the Harm Principle's Breaking Point," Ohio State University Journal of Criminal Law, Vol. 10 (2013), p. 685, at http://ailadc.org/form.php?form_id=12; Joel Feinberg & Robert P. George, "Crime and Punishment: Moralistic Liberalism and Legal Moralism: Harmless Wrongdoing: The Moral Limits of the Criminal Law," Michigan Law Review, Vol. 88 (1990), p. 1415.

99. US Dept. of Commerce, *Internet Policy Task Force, Copyright, Creativity and Innovation in the Digital Economy,* (Jul. 2013).

100. Nina Persak, Criminalizing Harmful Conduct: The Harm Principle, Its Limits and Continental Counterparts, Springer Science & Business Media, 2007.

101. The "harm" principle is fundamental to John Stuart Mill's approach to justifying or rejecting the intervention of the state through criminal law to prohibit, deter and punish certain behaviors. In *On Liberty,* Mill argues for "one very simple principle, as entitled to govern absolutely the dealings of society with the individual in the way of compulsion and control." That principle is that "The only purpose for which power can be rightfully exercised over any member of a civilized community, against his will, is to prevent harm to others. His own good, either physical or moral, is not a sufficient warrant," John Gray & G.W. Smith (eds.), *J.S. Mill on Liberty,* (New York: Routledge, 2003), p. 90.

102. The principle is captured by the Latin dictum *"actus reus non facit reum nisi mens sit rea"* ("the act is not culpable unless the mind is guilty"). *See, e.g.,* Oxford Reference.

103. *See, e.g.,* "Cyberla Tracker," UNCTAD, at http://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx.

104. For instance, while an early leader in the field of data protection, the US Privacy Act 1974 (USC Title 5, § 552a) applies only to the Federal Government, and subsequent laws applies to specific sectors, but there is no comprehensive law to date.

105. "What Is Data Protection?," Privacy International, at https://www.privacyinternational.org/node/44.

106. UN General Assembly, *Universal Declaration of Human Rights,* (10 Dec. 1948) 217 A (III) [hereafter, "UDHR"], at http://www.refworld.org/docid/3ae6b3712c.html.

107. UN General Assembly, *International Covenant on Civil and Political Rights,* (16 Dec. 1966) United Nations, Treaty Series, Vol. 999, p. 171 [hereafter, "ICCPR"], at http://www.refworld.org/docid/3ae6b3aa0.html.

108. OAS, *American Convention on Human Rights,* (22 Nov. 1969), at http://www.refworld.org/docid/3ae6b36510.html.

109. UN General Assembly, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, (10 Aug. 2011) A/66/290, para. 10, at http://www.ohchr.org/Documents/Issues/Opinion/A.66.290.pdf.

110. UNODC Cybercrime Study, *supra* § 1 C, note 7 at 110.

111. *See, e.g.,* "Brief History of the Internet," Internet Society, at http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet.

112. "Freedom of Expression Rapporteurs Issue Joint Declaration Concerning the Internet," R50/11 (1 Jun. 2011), pt. 1(c), at http://www.oas.org/en/iachr/expression/showarticle.asp?artID=848.

113. *Ibid.*

114. UN Human Rights Council, "Promotion, Protection and Enjoyment of Human Rights on the Internet," (32nd Session) [hereafter, "UNHRC Internet Resolution"], A/HRC/32/L.20 (27 Jun. 2016), at https://documents-dds-ny.un.org/doc/UNDOC/LTD/G16/131/89/PDF/G1613189.pdf?OpenElement.

115. UN General Assembly, "Calling of an International Conference on Freedom of Information," 59(I) (14 Dec. 1946), at https://documents-dds-ny.un.org/doc/RESOLUTION/GEN/NR0/033/10/IMG/NR003310.pdf?OpenElement.

116. Abid Hussain, Report on the Mission to the Republic of Korea of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, 1995 Report to the UN Commission on Human Rights E/CN.4/1996/39/Add.1 (21 Nov. 1995), at http://hrlibrary.umn.edu/commission/country52/39-add1.htm.

117. "Access to Information: An Instrumental Right for Empowerment," Article 19 & ADC, (Jul. 2007), p. 5, at https://www.article19.org/data/files/pdfs/publications/ati-empowerment-right.pdf.

118. *See, e.g.,* American Bar Association (ABA), "Part I: What Is the Rule of Law," at https://www.americanbar.org/content/dam/aba/migrated/publiced/features/Part1DialogueROL.authcheckdam.pdf.

119. *See, e.g.,* Operations Policy & Country Services (OPCS), "Dealing with Governance and Corruption Risks in Project Lending Emerging Good Practices," World Bank, (Feb. 2009), p. 7, at http://siteresources.worldbank.org/EXTGOVANTICORR/Resources/3035863-1281627136986/EmergingGoodPracticesNote_8.11.09.pdf.

120. *See, e.g., Commission v. Hungary, supra* note 74.

121. *See, e.g.,* Budapest Convention, *supra* § 1 B, note 32, at Art. 15.3.

122. "Access to Information Laws: Overview and Statutory Goals," Right2info, (20 Jan. 2012), at http://right2info.org/access-to-information-laws.

123. WDR, *supra* § 1 A, note 10, at 222.

124. *Ibid.*

Referenced in: § D. Framework for a Capacity-building Program

1. WDR, *supra* § 1 A, note 10, at 28 *et seq.* *See also* "World Internet Usage and Population Statistics," Internet World Stats, (4 Mar. 2017), at http://www.internetworldstats.com/stats.htm.

2. In Uganda, which has 22.6 million mobile phone numbers, there may be more mobile phones than lightbulbs. See Laura Gray, "Does Uganda Have More Mobile Phones Than Light Bulbs?," BBC News, (25 Mar. 2016), at http://www.bbc.com/news/magazine-35883649. Mobile phones are frequently used to make payments in remote rural areas: Across Africa, more than 25 million active users are reported to use "M-Pesa" ("M" for "mobile" and "Pesa" for "money" in Swahili), a means for making small-value payments from ordinary mobile. *See* "Vodafone M-Pesa Reaches 25 Million Customers Milestone," Vodaphone, (25 Apr. 2016), at https://www.vodafone.com/content/index/media/vodafone-group-releases/2016/mpesa-25million.html. *See also* "M-Pesa Transactions Rise to Sh15bn Daily after Systems Upgrade," (8 May 2016), at http://www.nation.co.ke/news/MPesa-transactions-rise-to-Sh15bn-after-systems-upgrade/1056-3194774-llu8yjz/index.html (noting that daily M-Pesa transactions in Kenya exceed Sh15bn (~US$145m)); Ignacio Mas & Dan Radcliffe, "Mobile Payments Go Viral M-PESA in Kenya," Capco Journal of Financial Transformation, Vol. 32 (2011): 169–82.

3. *Cf.* §§ 2 A & 2 B, below.

4. *Cf.* § 2 E, discussing e-evidence.

5. *See, e.g.*, CyberCrime@IPA, *Article 15 Conditions and Safeguards under the Budapest Convention on Cybercrime: Discussion Paper with Contributions by Henrik Kaspersen (Netherlands), Joseph Schwerha (USA), Drazen Dragicevic (Croatia)*, (Strasbourg: CoE, 2012) [hereafter, "Article 15 Safeguards"], at https://rm.coe.int/CoERMPublicCommonSearchServices/isplayDCTMContent?documentId=090000168030319 4#search=cybercrime%202467%20safeguards%2029mar12.

6. *Cf.* §§ 5 A & 5 B, generally, for a discussions of safeguards and human rights issues.

7. UN Development Programme (UNDP), *Human Development Report 2001: Making New Technologies Work for Human Development*, (New York: United Nations, 2001), at http://hdr.undp.org/en/content/human-development-report-2001. *See also* WDR, *supra* § 1 A, note 10, at 42 *et seq.*

8. *See* WDR, *supra* § 1 A, note 10, at 222 *et seq.*

9. For instance, in the fight against fraud and corruption, a "culture of compliance" has been espoused as a necessary element in rooting out corruption. *See, e.g.*, "Eight Ways to Move Toward a Culture of Compliance," Wall Street Journal, (7 Jul. 2013), at http://deloitte.wsj.com/cfo/2013/06/07/toward-a-culture-of-compliance-eight-initiatives-ccos-can-lead/.

10. For additional resources and examples, *see, e.g.*, CyberCrime@EaP, *Cybercrime and Cybersecurity Strategies in the Eastern Partnership Region*, (Bucharest: CoE, 2015), at https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016803053d2.

11. For references and links to domestic cybercrime legislation, *see* appendix 9 C.

12. *United States v. Chenault*, 844 F.2d 1124, 1131 (5th Cir. 1988).

13. Bettina Weisser, "Cyber Crime—The Information Society and Related Crimes," at, http://www.penal.org/sites/default/files/files/RM-8.pdf. *Cf.* computer fraud, which requires specific intent. USC Title 18 § 1030; fraud and related activity in connection with computers USC Title 18, § 1030(a)(4).

14. For additional resources and examples, *see, e.g.*, Budapest Convention, *supra* § 1 B, note 32, at Art. 15; CoE, *Explanatory Report to the Budapest Convention*, (23 Nov. 2001) [hereafter, "Budapest Explanatory Report"], at https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168008cce5b; "Country Profiles on Cybercrime Legislation," CoE, at http://www.coe.int/en/web/cybercrime/country-profiles; "Data Protection," CoE, at http://www.coe.int/en/web/data-protection/home.

Foundational Considerations

This chapter provides an overview for some of the foundational issues discussed in greater detail in the Toolkit. It starts by describing what is meant by "cybercrime", discusses what conduct is criminalized and then provides some "basics" regarding procedural, evidentiary, jurisdictional and institutional issues.

In this Chapter

A. Working Definition of Cybercrime

Table of Contents

Introduction

Broadly speaking, "cybercrime" encompasses illegal activities committed in cyberspace that either use ICT systems to commit the crime,[1] or that target ICT systems and the data that they store.[2] In the former category, ICT—be it a computer, smart phone or other device(s)—is a vital component of the offense's *modus operandi*.[3] Though vague and vast, such definitional variability is not necessarily detrimental, as technology's constant development requires an evolving definition of "cybercrime": a loose and flexible understanding of the term facilitates combatting illegal activities.[4]

Recognizing that a tight, globally-accepted definition of cybercrime does not exist,[5] this section **(I)** explores ways in which cybercrime has been understood, then goes through both **(II)** existing definitions of cybercrime as well as **(III)** grouping activities constituting cybercrime and **(IV)** finishes by proposing a working definition of "cybercrime" that will be used in the Toolkit. Discussion focuses on various approaches used by various institutions and organizations with an yet to looking to lessons learned from existing knowledge.

I. Defining Cybercrime

Different definitions of cybercrime, of varying breadth and depth, have been put forward by experts, industry and academia, some of which have been used by governments.[6] Under rule of law principles, it is understood that laws must clearly define prohibited behavior[7] and should be construed narrowly[8]; such tenets, or so-called canons of construction, are particularly true of criminal laws, where the consequences of misbehavior have significantly greater costs for perpetrators.

In order to define "cybercrime", it is helpful to begin **(A)** by defining a few key terms, before moving on **(B)** to consider technology's place in this evolving term and space and **(C)** to understand where cybercrime actually takes place. The subsection goes on to explore both **(D)** broad and narrow understandings of cybercrime before concluding with **(E)** a discussion of how and why national and international approaches differ.

A. Key Terms

Before further examining different definitions of "cybercrime", it is useful to describe some key elements central to construing cyberspace, namely "computer" (and "ICT"), "data" and "systems".[9] For the purposes of this Toolkit, these terms are understood as follows:

Computer

"***Computer***" is understood as an electronic device for storing and processing data. While those processes are typically in binary form, according to instructions given to it in a variable program,[10] it is expected that, in the not-so-distant future, devices may operate in quantum form using what are known as "quibits" (as opposed to "bits"), which, in essence, take the operating of binary form to a multidimensional level (*see* section 1 C, box 1.3, above). Relatedly, "***information and communications technology***" (**ICT**) is a broader term, which, though less commonly used to define cybercrime, emphasizes the place of

unified communications, and which integrates audio-visual, telephone and computer networks; although no concrete or universal definition exists as the concept continues to evolve with great rapidity, it can be understood as including computer systems and networks, as well as the data processed by them.

Data

"***Data***" (be it described as computer, ICT, information or electronic) describes a representation of facts, information or concepts that can be read, processed or stored by a computer or a computer system. Although some (though not all[11]) multilateral instruments explicitly provide that "computer data" includes computer "programs",[12] in practice all activities involving data are generally considered to be covered by provisions for computer data.[13]

System

"***System***" (be it described as computer, ICT, information or electronic) means any device capable of processing data. Some multilateral instruments define "computer network" as an interconnection between two or more computer systems.[14] In practice, "computer system" includes, but is not limited to, the linking of any number of computers, smart phones, tablets and other such ICT devices.[15]

B. Technology's Place: Now and to Come

At the heart of the matter of cybercrime is technology, both **(1)** as it stands now, both as a tool and as a target for cybercrime, and **(2)** as improvements come usher in both new opportunities and corresponding threats.

1. Today's Technological Infrastructure: A Tool & Target for Cybercrime

In defining cybercrime, it is helpful to have an understanding of the infrastructure allowing it, namely of the technology that underpins it. Technology plays a defining role in cybercrime.[16] On the one hand, and as discussed earlier,[17] technology, in the form of electronic devices (*e.g.*, computers or smart phones), or software (*e.g.*, viruses and malware) may be used to facilitate a diversity of crimes. Those crimes may be perpetrated against individuals, organizations or governmental entities. Essential cybertools having legitimate and beneficial uses—including high-speed internet, peer-to-peer file sharing and encryption—can be used to both enable and conceal criminal activity.

On the other hand, the technology itself may be the target of the crime. That technology needs to be understood in all of its diversity, being both hardware and software, and as being used by both the public and private sectors, as well as by organizations and individuals. Hardware is used by governmental and quasi-governmental authorities to assure the functioning of societies, from the functioning of power grids to the operating of dams and other pieces of infrastructure, to the

coordinating of traffic controls and emergency services. Software is used to assure communications, delivery of goods and monitoring of financial markets and delivery of its products. As the WannaCry cyberattacks demonstrate (*see* section 1 C, box 1.2, above), much of modern society has come to rely on ICT and systems' networking, making lives easier, while also making the elements of the infrastructure targets for attack.

Regardless of whether technology is understood as a facilitator or as a target in cybercrime, it bears noting that physical technology stores both the fruits and the evidence of cyber-committed crimes.[18] The nature of that evidence, as well as concerns such as the handling of e-evidence, is discussed in greater depth further on (*see* section 2 D, below).

It also bears noting that there is a great range and variance in the uses of technology in cybercrime. Certain cybercrimes require more technological *savoir-faire* or more powerful digital technologies in order to be carried out.[19] For instance, "point-and-click" crimes, such as downloading child pornography or engaging in cyberstalking require relatively minimal technological support. By contrast, phishing, identity theft and "denial-of-service" (DoS) or "distributed denial-of-service" (DDoS) attacks presuppose a much deeper and better understanding of digital and electronic technologies (*see* section 2 B, box 2.1, below). Deviant acts requiring greater technological know-how also tend to be more deeply embedded in the virtual world.

2. New Threats & Opportunities: "To Infinity and Beyond"[20]

Technological developments have led at once to new opportunities as well as to new threats and complexities. Although it is impossible to know what the future holds, it is important to consider what certain developments might mean. The start of that transformation is already being seen in the so-called "internet of things" (IoT), which, perhaps best defined as "the infrastructure of the information society",[21] is already revolutionized society and ways of life by (increasingly) optimizing device functionality and connectivity, creating new revenue opportunities and lowering operational costs through the inter-connection of all manner of smart devices.[22] These devices—including, for instance, household machines, heating, ventilation and air conditioning (HVAC) systems and the global positioning systems (GPS) of automobiles—are typically less secure than computers,[23] and yet, collectively, these devices result in an unprecedented sharing of vast volumes of sensitive data, therein raising serious security and privacy concerns.[24]

Technological developments will continue to transform the meaning of the internet and of interconnectivity. The "internet of everything" (IoE), a step beyond the IoT, is set to dramatically expand the present understanding of what makes the "infrastructure" of the information society. With the addition of the "smart" moniker to (potentially) everything, networking will involve not only devices but also the data on them,[25] and will also extend to directly connecting humans, both at the individual and collective level.[26] Anticipated advances—such as quantum computing,[27] biocomputing,[28] machine learning (or "pattern recognition"),[29] AI and autonomous systems—will both enhance and challenge today's norms—for instance, by rendering existing encryption

technology outmoded, prompting the development of "unbreakable" encryption.[30] While the ramifications of these concerns are, in their concreteness, beyond the scope of the Toolkit, it bears noting that anticipated technological advances promise to simultaneously revolutionize cyber-securitization and to facilitate more sophisticated cybercrime. This dramatic redefining of society at all levels makes the readying of systems' interoperability among states today, not tomorrow, all the more important.

C. Locating the Crime

The borders and physicality of the "real", physical world are nonexistent in the "virtual", digital world of cyberspace. Cyberspace enables criminals to impudently disregard borders and jurisdictions, to target large number of victims, and to do so both simultaneously and instantaneously. Although law-making and law-enforcing authorities, threatened by the new environment of cyberspace,[31] attempt to impose or imprint a Westphalian nation-state conception of sovereignty and jurisdiction upon cyberspace, the idea of a "border" is vague at best, and largely defies definition.[32]

That said, physical elements do play a mediating role between the physical and the virtual world, giving cybercrime a "location" that has underlying physical qualities to the more easily discernible virtual ones.[33] Recently, and increasingly, the physicality mediating access to cyberspace has moved beyond use of a computer or some other directive piece of ICT to integrative networking of smart devices, including cars, home utilities and wearable technology.[34] Indeed, smart cities[35]—and even networked cities[36]—are already becoming a reality. While cyberspace "radically subverts a system of rule-making based on borders between physical spaces",[37] these physical elements have been central to tying cybercrime into traditional legal understandings.

Although the complexities of jurisdictional issues is discussed in greater depth further on (*see* section 2 E, below), several points are worth raising here briefly. States typically exercise both their jurisdictional power and apply their laws to offenses committed on their territory. Cyberspace, however, transcends geographical frontiers, enabling perpetrators to act illegally in one state while being physically located in another state. In cases where the crime is enacted from abroad, jurisdiction is asserted on the basis that the committed offense negatively impacted the state (or its citizen). However, while such harm might be used as a means of establishing jurisdiction, the typical baseline for a custodial state to recognize, validate and accept the jurisdictional exercise of the requesting state is instead that of "double criminality" (or "dual criminality"), meaning that the perpetrator's comportment is punishable in both states.[38] This approach both respects the maxim of *nulla poena sine lege* ("no punishment without law"), as well as typically raising fewer jurisdictional concerns.[39] This mutuality is generally the basis, for example, of extradition law.[40]

Alternatively, jurisdiction might be asserted on the basis that the instrumentality enabling the offense—be it bank, money services or other instrument—was located in the state intending to prosecute. In such an instance, a form of what is often called "long-arm" jurisdiction is being

exerted over the perpetrator, whereby the foreign jurisdiction reaches beyond its territorial expanse to claim jurisdiction.[41] In either instance, a basic, territorial approach and understanding to jurisdiction is at work.

Case 2.1: Smc Pneumatics (India) Pvt. Ltd. vs. Shri Jogesh Kwatra (OS) No. 1279/2001 (India)

In India's first case of cyber-defamation, Defendant was accused of sending "distinctly obscene, vulgar, filthy, intimidating, embarrassing, humiliating and defamatory" emails to Complainant's employer and to employer's subsidiaries around the world. Complainant filed suit for permanent injunction restraining Defendant.

The court accepted that Complainant had made a *prima facie* case, and, the aim and intention established, enjoining Defendant *ex parte* to, first, cease and desist in sending of further such emails, and, second, restraining him from publishing, transmitting or causing to be published any information in both the physical world and in cyberspace that was derogatory or defamatory or abusive of Complainant.

D. Broad & Narrow Understandings of Cybercrime

Approaches to criminalizing cybercrime have been largely disunited, resulting in a Balkanization of criminal laws rather than the creation of a single, international *corpus juris* of "cybercrime". On a practical level, the absence of a concrete definition is a matter of particular concern in cybercrime as opposed to traditional crimes given cybercrime's inherent trans-border and trans-jurisdictional nature.

In the absence of a concrete definition, law enforcement authorities have generally distinguished between two main types of internet-related crime:

1. **A narrow understanding of cyber-enabled crimes,** which focuses on advanced cybercrime (or high-tech crime), and which involves sophisticated attacks against computer hardware and software
2. **A broad understanding of cyber-enabled crimes,** which are so-called "traditional" crimes committed with the facilitation of ICT, or which are committed "in" cyberspace, and might include crimes against children, financial crimes, and even terrorism.[42] This binary understanding, which has permeated many systems, was introduced during the Tenth UN Congress on the Prevention of Crime and the Treatment of Offenders in 2000 as "cybercrime in a narrow sense" (or "computer crimes")[43] and "cybercrime in a broad sense" (or "computer-related crimes").[44]

E. National versus International Approaches

Defining cybercrime depends on the context and purpose for which the definition will be used. In national, domestic legislation, the purpose of defining cybercrime is to enable investigation and prosecution of various offences falling under that umbrella. As such, it may not be useful to define the term either narrowly or precisely, especially when procedural provisions of domestic law could be applicable to acts constituting cybercrime as well as other crimes involving e-evidence.[45] In the international context, defining cybercrime is useful for interpreting provisions concerning cross-border investigative powers. Some multilateral treaties on cybercrime extend international cooperation rules "for the collection of evidence in electronic form of a criminal offence",[46] while others specify that international cooperation rules apply to differentiate between "offences against computer information"[47] and "cybercrime".[48] This differentiation has led the United Nations Office on Drugs and Crime (UNODC) to note that "[i]n the international sphere, conceptions of 'cybercrime' may thus have implications for the availability of investigative powers and access to extraterritorial e-evidence."[49]

That is not to understate the link between national laws and international instruments. To illustrate, note that many concepts in the Budapest Convention draw from national legislations.[50] In turn, countries ratifying the Budapest Convention have utilized the Convention's understanding of cybercrime within their own national laws. This dual integrativeness has helped reduce the friction among national laws, which in turn, improves state coordination and provides clarity through convergence.

II. Existing Definitions

This section briefly takes stock of selected practices in definitional approaches to "cybercrime" as used **(A)** in domestic, national legislation, **(B)** in multilateral instruments on cybercrime and **(C)** in the literature.

A. National Level

While a number of countries have legislation dealing with cybercrime,[51] only a few countries define "cybercrime" in their national legislation.[52] Of those countries with a national cybercrime law, only a few explicitly use the term "cybercrime" in the articles of such law.[53]

Rather, titles or provisions in national laws pertaining to cybercrime use terms such as:

- "Electronic crimes"
- "Computer crimes"

- "Information technology crimes"
- "Crimes in the sphere of computer information"[54]
- "High-technology crimes"[55]

Many other jurisdictions construe cybercrime as a crime committed with the use of ICT.[56]

Regardless of how cybercrime is addressed, or what method is used to adapt it, a legal definition of "cybercrime" is rarely provided. Even when domestic legislation explicitly refers to "cybercrime", there are often differences in how various national laws of the same state define the term. For example, while one approach defines cybercrime as "crimes referred to in this law",[57] another approach is to do so on the basis of instrumentalities, broadly defining cybercrime as "criminal offences carried out in a network or committed by the use of computer systems and computer data".[58]

B. International & Regional Instruments

There is no multilateral cybercrime instrument that explicitly defines the meaning of term. That said, the term has been used to accommodate a broad range of different offences, making any typology or classification difficult[59]: "[t]he word 'cybercrime' itself is not amenable to a single definition, and is likely best considered as a collection of acts or conduct, rather than one single act".[60]

There are, however, two general approaches within applicable multilateral instruments on cybercrime on how to conceptualize cybercrime:

1. **The first approach** understands cybercrime as a collection of acts, without actually providing a singular definition of the term "cybercrime" itself;
2. **The second approach** is to offer a broad definition of either the term "offences against computer information"[61] or to use the term "information crime"[62] without explicit reference to the term "cybercrime".

Examples of the first approach can be found, in the Budapest Convention, the AU Convention and the ECOWAS Directive. Examples of the second approach are found in the CIS Agreement[63] and the SCO Agreement.[64]

C. Academia

Although academia has made wide and varying contributions to the effort to create a definition of "cybercrime",[65] no single, standardized consensus definition has been agreed upon. One colorful descriptor is that of cybercrime as "new wine, no bottles".[66] In any case, similar to what has been just discussed, there is consensus that cybercrimes can be appropriately understood as including both traditional crimes moved to a new environment, also new crimes made possible by this new

environment.[67] This understanding has let one author to classify according to "issues of degree" and "issues of kind".[68] Such variance in the definition of cybercrime is in part due to the rapid advances and evolutions in ICT, as well as understandings of cyberspace.[69]

III. Classifying Cybercrime

While specific cybercrimes will be considered hereafter (*see* section 2 B, below), it is worth considering how different regimes have classified cybercriminal behavior in developing an understanding of cybercrime. In the absence of a unitary definition, and without any unitary concept of what cybercrime is, the term is better understood as a range of acts falling into a certain category of crimes.[70] That said, while a classification or categorization of cybercrime is less contentious, it is nonetheless difficult to find consensus with regard to the appropriate divisions of acts constituting cybercrime in domestic legislation, multilateral instruments or the literature.[71] Herein, seven different classifications, as laid out in international instruments are considered, namely, those of **(A)** the UN Secretariat, **(B)** COMSEC, **(C)** the AU; **(D)** the ECOWAS, **(E)** UNODC, **(F)** UNICRI and **(G)** the CoE.

A. United Nations Secretariat

The UN Secretariat carries out the diverse day-to-day work of the United Nations, servicing the other principal UN organs and administering their programs and policies. The Secretariat's activities include administering peacekeeping operations, mediating international disputes, surveying economic and social trends and problems and preparing studies on human rights and sustainable development.[72] In a background paper for a workshop on cybercrime presented at the Thirteenth UN Congress on Cybercrime Prevention and Criminal Justice in 2015, the UN Secretariat, building on its earlier documentation,[73] took a binary approach to defining cybercrime.

Under the UN Secretariat's approach, cybercrime is categorized according to the nature of the offense:

1. Offenses affecting the confidentiality, integrity and availability of computer data or systems; and
2. Offenses where computer or ICT systems form an integral part of the crime's *modus operandi*.[74]

B. Commonwealth Secretariat

COMSEC is the main agency and central institution of the Commonwealth of Nations,[75] an intergovernmental organization of fifty-three Member States that were mostly territories of the

former British Empire.[76] COMSEC facilitates cooperation between members, organizes meetings, assists and advises on policy development and provides assistance in implementing decisions and policies of the Commonwealth.[77] In its 2014 Report to Commonwealth Law Ministers, COMSEC provides that "cybercrime" is not a defined legal category but rather a label that has been applied to a range of illicit activities associated with ICT and computer networks.[78]

The Report also categorizes cybercrime in a binary fashion:

1. New, criminal offences covering conduct that is harmful to ICT; and
2. Traditional crimes committed using, or affected by, ICT.[79]

C. African Union

Established in 2000[80] with the vision of "[an] integrated, prosperous and peaceful Africa, driven by its own citizens and representing a dynamic force in global arena",[81] the AU plays an important role in international cooperation. The AU is part of a series of initiatives going back to 1980 that had the continent's economic and social development as their quest.[82] In 2014, the AU adopted its Convention on Cyber Security and Personal Data Protection.[83] The tripartite Convention speaks to electronic transactions, personal data protection and promoting cyber security and combatting cybercrime.[84]

The AU Convention classifies cybercriminal offenses in two:

1. Offences specific to ICT[85]; and
2. ICT-adapted offenses.[86]

D. Economic Community of West African States

Founded in 1975, ECOWAS is a regional group of fifteen West African countries[87] headquartered in Abuja, Nigeria with the mandate of promoting economic integration among its constituents.[88] An important regional bloc, ECOWAS is one the five regional pillars of the African Economic Community (AEC).[89] In working towards that integration, ECOWAS has considered the matter of cybercrime, and has produced its "Directive on Fighting Cyber Crime within ECOWAS".[90]

The ECOWAS Directive categorizes cybercrimes in a binary manner:

1. New crimes; and
2. Traditional, ICT-adapted crimes.[91]

It bears noting that only the intended objectives of ECOWAS directives are binding on its Member States, and that each Member State retains the freedom to decide on the best strategies for implementing and realizing those objectives.[92]

E. United Nations Office on Drugs and Crime

UNODC is mandated to assist UN Member States in their struggle against illicit drugs, crime and terrorism.[93] This mandate is in support of the Millennium Declaration made by Member States, in which they resolved to intensify efforts to fight transnational crime in all its dimensions, to redouble the efforts to implement the commitment to counter the world drug problem, and to take concerted action against international terrorism.[94] UNODC is built on the three pillars of (1) field-based technical cooperation projects to enhance Member State capacity to counteract illicit drugs, crime and terrorism; (2) research and analytical work to increase knowledge and understanding of drugs and crime issues and to expand the evidence base for policy and operational decisions; and (3) normative work to assist states in the ratification and implementation of the relevant international treaties, the development of domestic legislation on drugs, crime and terrorism, and the provision of secretariat and substantive services to the treaty-based and governing bodies.[95]

Taking a slightly more complicated approach to categorizing cybercrime, UNODC posits three, non-exhaustive categories in its *Comprehensive Study on Cybercrime*[96]:

1. Acts against the confidentiality, integrity and availability of computer data or systems;
2. Computer-related acts for personal or financial gain or harm, including sending spam; and
3. Computer content-related acts.[97]

F. United Nations Interregional Crime and Justice Research Institute

UNICRI exists to assist the international community in formulating and implementing improved crime prevention and criminal justice policies through action-oriented research, training and technical-cooperation programs. Having launched a strategic engagement in technology to support the fight against crime and responding to the misuse of technology, UNICRI is working to maintain a harmonized approach that effectively balances security concerns and human rights.

Similar to UNODC, UNICRI posits a tripartite classification of cybercrime in its "Cybercrime: Risks for the Economy and Enterprises" Roundtable in 2013[98]:

1. Cyber analogues of traditional crimes;
2. Cyber publishing of illegal content (*e.g.*, child pornography; incitement to racial hatred); and
3. Crimes unique to cyberspace (*e.g.*, denial of service and hacking).[99]

G. Council of Europe

Founded in 1949, and with forty-seven Member States and six Observer States,[100] the CoE has the purpose of "achieving a greater unity between its members for the purpose of safeguarding and realizing the ideals and principles which are their common heritage and of facilitating their economic and social progress".[101] With a focus on promoting human rights, democracy, rule of law, economic development and integration of certain regulatory functions in Europe,[102] the Council has developed a diversity of treaties and explanatory reports.[103]

Most notable for the purposes at hand is the CoE's Convention on Cybercrime, commonly known as the "Budapest Convention".[104] The first global instrument on cybercrime, the Convention's main objective is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially through the adoption of appropriate legislation and by fostering international cooperation.[105] Focusing on infringements of copyright, computer-related fraud, child pornography and violations of network security,[106] the Convention operates on the aspiration of legal harmonization and, accordingly, seeks and sets the highest international level of agreement. The Convention details powers and procedures, such as for searching computer networks and lawful interception to that effect, all to address both the crimes listed in the Convention and any other crimes entailing e-evidence.

The Budapest Convention proposes the most nuanced categorization of cybercrime all major instruments, dividing cybercrime into four different types of criminal behavior:

1. Offenses against the confidentiality, integrity, and availability of computer data and system[107];
2. Computer-related offenses[108];
3. Computer content-related offenses (defined as child pornography)[109]; and
4. Computer-related offenses involving infringements of copyright and related rights.[110]

The Convention also allows for ancillary liability and sanctions for inchoate offenses (attempt, and aiding or abetting)[111] and for corporate liability.[112]

Conclusion: The Toolkit's Working Definition of "Cybercrime"

A precise definition of "cybercrime" does not exist. Broadly speaking, cybercrime is understood as a "computer-related crime" and need not necessarily target a computer or ICT device.[113] A "typology" approach of acts constituting cybercrime has been used by a number of institutions and agreements, including in the AU Convention,[114] the ECOWAS Directive[115] and COMSEC's 2014 report to Commonwealth Law Ministers.[116]

Instead of categorizing, and, in an effort to make the Toolkit as useful as possible, a broad and expansive working definition of cybercrime is used herein. Accordingly, the term "***cybercrime***" is understood to include *criminal conduct (as provided in substantive law) directed against the confidentiality, integrity and availability of ICTs, as well as criminal acts carried out through the instrumentality of ICTs.*

Relatedly, the term "***ICT***", a term growing in usage, is understood to include *computer systems and networks, as well as the data stored and processed thereon.* Using the term "ICT" as opposed to computer is helpful as it reflects recent trends in technological developments, including convergences of older forms of technologies with newer ones.

B. Criminalized Conduct

Table of Contents

Introduction

As developed in the previous section,[1] the Toolkit uses a broad definition of *"**cybercrime**", understanding it as criminal conduct (as provided in substantive law) directed against the confidentiality, integrity and availability of ICTs, as well as criminal acts carried out through the instrumentality of ICTs.* That definition construes cybercrime as including both information and systems as targets (ICT-targeted), and the use of ICT devices to conduct criminal offenses (ICT-enabled offenses). Building upon the previous section's definition, this section examines criminalized conduct. While the working definition is bipartite, this section presents criminalized conduct, without trying to classify that behavior as either ICT-targeted or ICT-enabled—indeed, some will be both.

Additionally, as much as already been written about them, this section does not attempt to cover all of the well-accepted cybercrimes, but is instead intended to focus on select new and emerging

issues, as well as to shed new light on some of those more well-known cybercrimes. One of the great challenges in combatting cybercrime is "future-proofing" the law—ensuring that the law keeps pace with all sorts of new ways to conduct criminal activity on-line. In practical terms, one question facing policy-makers and legislators is whether to attempt to specifically criminalize each new type of activity, or to craft a legal framework that is more general in nature but flexible enough to ensure that it can be applicable to new sorts of criminal activity as they arise.

Just as with the definition of cybercrime, it is equally difficult to find consensus on what constitutes cybercrime beyond a limited, core number of acts compromising ICT confidentiality, integrity and availability. With the exception of ICT-facilitated dissemination of child pornography,[2] there is little agreement on what constitutes content-related offences.[3]

This section runs through several of the mostly commonly criminalized acts constituting cybercrime: **(I)** unauthorized access to a computer system (or "hacking"), **(II)** unauthorized monitoring, **(III)** data alteration (or data "diddling"), **(IV)** system interference, **(V)** computer content-related offences, **(VI)** cyberstalking, **(VII)** financial cybercrimes and **(VIII)** misuse of devices. It concludes in an integrative attempt to prepare the discussion on procedural issues, discussed more thoroughly in the next section (*see* section 2 C, below).

I. Unauthorized Access ("Hacking")

The unauthorized access to an ICT system—commonly known as "hacking—, is, in many ways, the most basic cybercrime as it enables subsequent (cyber)criminal behavior.[4] Once access is gained to an ICT device or network, the cybercriminal may target information and data, or may turn to target systems. There are various means for infiltrating a device, system or network. "Malware" is an umbrella term used to describe malicious code or software, including viruses, worms, Trojan horses, ransomware, spyware, adware and scareware.[5]

Box 2.1: Various Hacking Techniques

Hacking might be accomplished through a variety of techniques. The most common forms include the following:

Malware: A malicious piece of code (including viruses, worms, Trojans or spyware) which infects devices or systems, which is typically capable of copying itself, and which typically has a detrimental effect, such as corrupting the system or destroying data.

Adware: A malicious piece of code that downloads or displays unwanted ads when a user is online, collects marketing data and other information without the user's knowledge or redirects search requests to certain advertising websites.

Social Engineering: The deceptive use of electronic communications, such as emails or social media messages, for purposes of fraud, system access or collecting sensitive information; the most common forms of social engineering includes phishing, pretexting, baiting, *quid pro quo* and tailgating.[6]

Botnet: A network of private computers infected with malicious software and controlled as a group without their owners' knowledge in order to multiply the effects of cyberattack.

Denial-of-Service (DoS) or Distributed Denial-of-Service (DDoS) Attack: An attempt to overwhelm or overload an organization's website or network in order to render it unavailable to intended users by interrupting or suspending services.

Ransomware: Malicious code disguised as a legitimate file used by hackers to encrypt data on users' devices, thereby preventing access to either the data or to the device itself until a ransom fee is paid. The inverse of a DoS attack, ransomware makes it impossible for the user decrypt his or her its own data without the decryption key, which (in principle) is offered upon payment of a ransom.

Injection Attack: The most common and successful attack-type on the internet (*e.g.*, SQL Injection (SQLi), Cross-Site Scripting (XSS)), it targets web-based applications, and works by hiding malicious code (a "payload") inside verified user input (thereby bypassing authentication and authorization mechanisms) that is shown to the end-user's browser, which in turn executes the apparently trustworthy script. The script often creates errors visible to the attacker, many of which tend to be sufficiently descriptive to allow an attacker to obtain information about the structure of the database and thereby control it.[7]

Hacking by definition compromises system integrity and, as such, imperils confidence not only in that individual device, system or network, but also potentially in the larger notion of the integrity of networking and cyberspace as a whole.[8]

Box 2.2: Target Corp. Targeted in Massive Data Hack

In December 2013, in one of the largest data breaches ever reported, hackers infiltrated the ICT systems of Target Corporation, the second-largest discount retailer in the United States, and stole personal information (email, addresses, etc.) of some seventy million customers, including credit and debit card records on more than forty million customers.

The Target breach, caused by malware installed on the company's networks that siphoned away customer information, happened during the holiday shopping period. When

announced, the chain's traffic, sales and stock value were immediately affected, with profits falling by forty-six percent for that quarter. Target subsequently agreed to pay US$10 million to settle a lawsuit brought by shoppers affected by the breach.

Since most ICT systems are usually shielded from unauthorized access, an intruder must penetrate the security system. As such, many legal systems class hacking—simply on the basis of being unauthorized access—as criminal in and of itself.[9] The Budapest Convention, for instance, addresses hacking by criminalizing "offenses against the confidentiality, integrity and availability of computer data and systems" at large,[10] and, more specifically, by targeting "illegal access", understood as "access to the whole or any part of a computer system without right".[11] Laws generally categorize the offense as unauthorized entry into a protected ICT system, regardless of the offender's purpose.[12] However, the Budapest Convention allows that further *mens rea* elements[13] in addition to intentionality and "without right" might be included, as State Parties "may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system".[14]

Case 2.2: United States v. Marcel Lehe Lazăr (USA)[15]

Defendant, Marcel Lehe Lazar, pled guilty to two of nine counts of an indictment that included three counts of gaining unauthorized access to protected computers, having hacked into email and social media accounts of some one hundred Americans, including family members of two former US Presidents, a former US Cabinet member, a former member of the US Joint Chiefs of Staff and a former presidential advisor. Lazar claims to have breached Hillary Clinton's personal email server,[16] although there is no evidence to verify that claim.

Lazar was apprehended and tried in his native Romania, where he was found guilty on similar charges and jailed for seven years.[17] Thereafter, in a showing of international cooperation among law enforcement authorities, he was extradited to the United States.[18] The US District Court for the Eastern District of Virginia sentenced him to a further seven years in prison.[19]

II. Unauthorized Monitoring

Just like hacking, unauthorized "monitoring"[20] might target devices, data or both; when data is targeted, it is often referred to as "illegal interception". Such activity is typically done by using or installing monitoring devices or software in the ICT system after having gained access to the system. The physical world analogue is wiretapping. It bears noting that, while initial access to the system

may have been granted and authorized, this offence is not in the unauthorized system entry—as in hacking—but rather in remaining "in" the system thereafter, and monitoring or otherwise affecting the system and/or any stored or transmitted data therein.[21] Thus, while authorized entry may not have been *per se* revoked (that is, if it had been granted), permission to remain in the system, even if only in a "viewing" capacity, has not been granted.

Box 2.3: Spotting Hack Attacks and Monitoring Malware

Edward Snowden, of renown for his unauthorized copying and leaking of classified information collected by the NSA in 2013,[22] is developing a smart phone case that will inform the user whether the device has been hacked.[23] As mobile phones are the "perfect tracking device",[24] and as it is relatively easy to develop software that masks whether the phone's integrity has been compromised, Snowden and a colleague are developing a phone-mounted battery case that monitors radio activity. Monitoring technology might be used as much by governments[25] as private sector spies.[26]

An example of monitoring malware is Flame (also known as well as Flamer, sKyWIper, and Skywiper),[27] a modular computer malware discovered in 2012 by Kaspersky Labs at the prompting of the ITU, the UN agency that manages information and communication technologies.[28] Flame, which may have been active for as long as eight or more years before it was discovered,[29] not only targeted computers running the Microsoft Windows operating system, but, in an act that broke world-class encryption, was found to have been delivered through Windows updates.[30] A precursor to the Stuxnet virus,[31] Flame was designed to stealthily search top-secret files and gather intelligence through keyboard, screen, microphone, storage devices, network, WiFi, Bluetooth, USB and system processes,[32] subsequently transmitting document summaries of the gleaned intelligence.[33] As network managers might notice sudden data outflows, the malware was designed to gradually transmit harvested information to its command-and-control server.[34] Data transfer could be done with any Bluetooth-enabled device, and, with a "Bluetooth rifle", could have a range of up to two kilometers.[35] Flame has been particularly used to target Middle Eastern countries.

III. Data Alteration

Data alteration (or data "diddling", or false data entry[36]), is the interception and changing of data before or during entry into a computer system, or the altering of raw data just prior to processing and then changing it back after processing has been completed.[37] It can occur at various points along the chain of information entry. However, as E2EE is growing in both effectiveness[38] and in frequency,[39] data diddling is increasingly happening by hacking the device before either the to-

be-sent data has been encrypted or after the received data and been unencrypted, rather than intercepting the data and then having to unencrypt it.[40]

As with many other cybercrimes, data diddling allows cybercriminals to manipulate output while largely preserving the perpetrator's anonymity; however, data diddling is often very subtle and virtually undetectable. Forging or counterfeiting documents are typical examples. Cyber forensic tools can be used to trace when data was altered, what that data was and then to change it back to its original form. A simpler and more direct method of control is through version control and by keeping multiple records, including hardcopies, just as much for comparison's sake as to back up the data. Data diddling may be used to target a wide-range of information; indeed, concern over possible tampering with public legal documents has limited governmental recourse to the web in areas as diverse as the publication of court judgments[41] and voting.[42]

Case 2.3: People of Colorado v. Raymond D. Ressin et al. (USA)[43]

In a matter going back to 1978, Defendants defrauded a brokerage firm of US$171,756.17, and were convicted on three counts of theft. Raymond Ressin, a clerk working for a brokerage firm in Denver, Colorado, purchased two hundred shares of Loren Industries at US$1.50 for his outside accomplice, Robert Millar, amounting to a total of US$300. He subsequently altered the account number suffix, changing the purchase from a legitimate "cash" account, which was to have been paid in full, to a "margin" account, which qualified the purchase for a loan of up to fifty percent of the account value. Ressin subsequently changed the last two digits of the authorization code from LII (Loren Industries, Inc.) to LILN (Longing Island Lighting), an approved margin stock worth US$130 a share. As a result, the account value went from US$300 to US$26,000, which, as a margin account, also came, with a borrowing power of US$13,000. Ressin subsequently adjusted the records inputted into a computerized accounting system. Repeating the process, and then leveraging that fraudulent borrowing power, Defendants made further purchases, parlaying the initial US$300 investment to a net value of US$171,756.17 (approximately US$700,000 in 2016).

IV. System Interference

As already discussed,[44] a fundamental interest is the "integrity" of private and public ICT systems and networks, meaning that they function according to their operating rules and the input furnished by the owners.[45] As any unauthorized interference can seriously undermine public trust in the secure, proper functioning of ICT systems, many legal systems have adopted criminal sanctions to punish it.[46] This kind of activity goes beyond undermining uncertainty in cyberspace and in the

systems constructed therein.[47] Typical examples include unauthorized transmission and changes of data, removal or destruction of data and of software, as well as impeding access to an ICT system.[48] Just as system interference (sometimes called "cybersabotage") can be conducted by either private industry or by governments, so, too, can its targets be either private industry or public operations. In this section, system interference is being discussed in the context of criminal gain.[49]

Box 2.4: Sony Pictures Entertainment Attacked

On 24 November 2014, a hacker group identifying itself as "Guardians of Peace" (GOP) leaked confidential data stolen from the film studio Sony Pictures Entertainment.[50] The large amount of leaked data included personal details on Sony Pictures employees and their families, emails between employees, information about executive salaries, copies of then-unreleased Sony films, and other information.[51] Following threats to release more information, Sony Pictures bowed to the demands by the GOP group not to release the film *The Interview,* a spoof on North Korean premier, Kim Jong-un.[52] US authorities concluded that North Korea had been "centrally involved" in the hack.[53]

V. Computer Content-related Offences

Computer content-related offences are acts of disseminating, making available or storing material with illegal content by the use of computer systems or the ICTs. Particular concern is given to content that is religiously or racially discriminatory, contains child pornography or incites hate acts or terrorism.

This category of offenses can often pose challenges to freedom of expression protections.[54] International law allows the prohibition of certain types of expression.[55] However, there are often disparities among domestic legislation. For example, the online dissemination of racist and xenophobic material is prohibited in many European countries, while the same acts might be protected in the United States.[56]

While most areas of cybercrime still lack consensus—especially for computer content-related activities—, cyber child pornography, in particular, is an area where criminalization is generally accepted. Although specific cyber-pornography laws are sometimes legislated,[57] such activity is more typically criminalized by expanding either the general criminal law[58] or the cybercrime law.[59] Amendments tend to make provisions general enough to cover both traditional and online renderings (*i.e.,* "by any means"),[60] or to make specific amendments explicitly speaking to online child pornography.[61]

VI. Cyberstalking

Cyberstalking is a crime that often blurs the line between the real and the virtual, and even between the physical and the psychological. As such, it deserves space to discuss **(A)** the concept of stalking and cyberstalking, **(B)** how best to combat cyberstalking at the societal level and **(C)** a brief *exposé* of the elements that go into good practice of prosecuting cyberstalking.

A. The Concept of (Cyber)stalking

Stalking is a pattern of behavior involving willful or intentional acts[62] which, though often individually inconsequential, collectively make the victim feel harassed, nervous, anxious, fearful, threatened or otherwise insecure.[63] Behavior amounting to stalking ranges from the repeated sending of unwanted messages (telephonic, mail or otherwise) or gifts, to the more aggressive activities of surveying or pursuing the victim. Stalking is committed by those with varying backgrounds, motivations and psychological disorders[64]; the majority of perpetrators have a problematic social life and may suffer from psychosocial problems or disorders, such as schizophrenia paranoid disorder. In the United States, an estimated 3.4 million persons aged eighteenor older were victims of stalking during any given twelve-month period.[65]

While a wide range of acts can be involved in stalking, and while they can result from a wide series of causes, two critical elements characterize stalking: first, the repetitiveness of the overall behavior (not necessarily any one type of act); second, the victim's reasonable perception of that behavior as unwelcomed and unacceptably invasive. Stalking itself does not involve the infliction of any direct physical harm by the perpetrator. Rather, antistalking laws operate as a means of providing law enforcement officials with a mechanism for intervening before violence actually occurs.[66]

Cyberstalking, the convergence of stalking and cyberspace, is characterized by the repeated use of unwanted electronic communications—emails, spamming, flaming, online defamation, blogging, and the like[67]—sent directly or indirectly, which renders the victim insecure, or which misrepresents the victim online. Just as with traditional stalking, it is the behavior's repetitiveness and the reasonable, subjective apprehension that characterize cyberstalking.

While the medium might be different, stalking done in the virtual world can be just as distressful, destructive and damaging as that done in the physical world. While cyberstalking may be complemented by physical-world stalking,[68] its effects can be far more destructive.

Case 2.4: Ramm v. Loong (Singapore)[69]

Leandra Ramm, a US citizen residing the area of San Francisco, California, was the victim of cyberstalking by Colin Mak Yew Loong, a Singaporean man, residing in Singapore. For six

years, Loong, who had initially posed as a director of a music festival, made harassing phone calls and sent some 5,000 emails, in addition to creating hate groups on Facebook and Twitter and a slanderous blog, through which he made threats of rape and physical violence against Ramm and her family. Loong even made bomb threats to the opera companies that engaged her. A promising opera singer, Ramm's career was destroyed and she suffered serious psychological episodes, including contemplating suicide, eventually being diagnosed with post-traumatic stress disorder (PTSD).[70]

For six years, Ramm was rebuffed by the FBI, the New York Police Department and other government agencies, and was met with a lack of interest by Singaporean authorities (where cyberstalking was not criminalized). Eventually, Ramm hired a cybercrime expert with links to the US Secret Service (USSS), who was able to navigate the US and Singaporean legal systems.

Eventually, Loong admitted to thirty-one counts of criminal intimidation between 2005 and 2011 (as well as confessing to having harassed two other foreigners (a Ukranian violinst and the German boyfriend of a Hungarian pianist) and a Singaporean business woman; to criminally trespassing at St. James Church; and to stealing biscuits from the Church's kindergarten. After considering the aggravating factors, the Singapore Subordinate Court determined that Loong made "vicious threats of violence and extremely vulgar email rants" against Ramm that was tantamount to "mental assault" as well as repeated acts of aggressive intrusion, and sentenced Loong to thirty-six months in prison (nine months jail for each of the fourteen counts, with four of the sentences running consecutively) and to pay a fine of S$5,000.[71]

Taking almost nine years, the conviction makes for the first successful prosecution of an international cyberstalking case.[72] In the words of the presiding judge, the case is "a timely reminder that harassment laws need to keep pace with changes in technology and the pervasive use of the Internet and social media". Singapore has subsequently criminalized cyber-bullying and -stalking.[73]

B. Combatting Cyberstalking at the Societal Level

Cyberstalking has only relatively recently been seen as a serious crime, and is still not universally criminalized. In 2014, a European Union-wide survey across the twenty-eight Member States found that only eleven had specific anti-stalking laws.[74] Since then, the CoE's Istanbul Convention has substantially worked to harmonize laws on violence against women across Europe, including stalking (without distinction between physical- and cyber-stalking).[75] In the United States, stalking became an issue of social concern in the 1990s[76]; the Violence Against Women Act (VAWA) criminalized stalking under US federal legislation.[77] The first jurisdiction in the United States to

criminalize cyberstalking was California in 1999[78]; thereafter, in 2000, language was added to the federal law, VAWA, to include cyberstalking.[79] While legal definitions vary across jurisdictions,[80] thereby complicating prosecution and investigation,[81] courts have facilitated legislative hiccups by extending existing, traditional statutes to include electronic tools.[82]

Case 2.5: United States v. Baker (USA)[83]

Defendants, Abraham Jacob Alkhabaz, a.k.a. Jake Baker, and Arthur Gonda, were prosecuted for electronic mail messages involving sexual and violent behavior towards women and girls. Baker also posted a reputedly-fictional story describing the torture, rape and murder of a young woman sharing the name of one of Baker's classmates at the University of Michigan.

Although the true identity and whereabouts of Gonda, who was operating from a computer in Ontario, Canada, are still unknown, Baker was arrested and charged under federal statute 18 USC § 875(c), which prohibits interstate communications containing threats to kidnap or injure another person. The count that had been based on Baker's story publication was dismissed as protected as free speech under the First Amendment of the US Constitution. The other charges, which were based on defendants' email correspondence, and thus of a private nature, were deemed not to constitute "true threats" by the district court. While the US Court of Appeals for the Sixth Circuit upheld the District Court's decision, it bears noting that just what constitutes a "true threat" under US law remains unclear.[84]

Cyberstalking is frequently misconstrued as a crime lacking significance. In order to effectively combat cyberstalking, the government must, first, build sufficient capacity in order to both conduct proper investigations and to offer alleged victims the appropriate degree of psychological support and understanding, and, second, actively work at breaking attitudinal barriers that make such behavior acceptable.

Overcoming attitudinal barriers is also a necessary part of crime fighting. In stalking at large, and in cyberstalking in particular, initial contact between perpetrator and victim is generally benign, and may even be positive. Once communications turn disturbing, however, there is a tendency of victims to immediately and spontaneously destroy the unwelcomed overtures; such behavior by victims is typically motivated out of a sudden onset of fear or embarrassment. Unfortunately, doing so can significantly hinder authorities in their investigating. As such, the battle against (cyber) stalking begins by breaking attitudinal barriers and educating people so victims are not oblivious to the signs of stalking and do not destroy evidence.

C. Examples of Good Practice in Prosecuting Cyberstalking

The first step to a successful prosecution is collecting sufficient information from the victim. If there are grounds to assume that the act was perpetrated by an acquaintance, investigators may have to focus on the victim's internet activity. The investigative process stands or falls on trust: investigators must give victims ground for putting trust and confidence in them, and for feeling secure enough in sharing their story, a story that can often be quite disturbing and which can become increasingly disturbing as more evidence is uncovered and the fuller pictures emerges.[85] Having established a rapport of trust with the victim and having heard the victim's account, investigators then need to secure actionable evidence. Having brought the incidences to the attention of law enforcement authorities, victims must be instructed in how to preserve subsequent communication and content; as digital evidence can be particularly fragile, (*see* section 1 D, below), attention to properly instructing victims should not be undervalued. Further, victims need to be instructed on how best to cooperate with investigators.

The anonymity of cyberspace often makes it difficult to identify a methodical cyberstalker who does not wish to be identified. Such is especially complicated by the fact that so many perpetrators have never had a relationship with the victim. Moreover, investigators usually face difficulties tracing suspects, as most cyberstalkers do not have material motivation. Technology has created a whole new space in which crime can occur, and technological developments continue to outpace anti-cyberstalking laws.[86] Such being the case, investigators need to be sufficiently trained and experienced in more than just psychology and standard evidence collection. For instance, familiarity should be had in dealing with different subscriber networks, including email, blogs and bulletin boards, text messaging and telephone and fax networks so as to understand how to piece together —and preserve—an evidence trail.

As with most cybercrimes, cyberstalking's frequently transnational, cross-boundary nature, as combined with technical advances that help perpetrators to remain anonymous, significantly increase the cost and timing of the combatting this crime. Indeed, the UK's Crown Prosecution Service has noted information request result in delays of up to three months, as compared to the apprehending of physical-world stalkers, which is usually completed within hours.[87] In addition to drawing out the duration of the crime, these delays also give perpetrators valuable time to destroy evidence.

VII. Financial Cybercrimes

From fraud to forgery, spoofing to spamming, cybercriminals have particularly targeted the financial services sector.[88] As such, it is worth discussing **(A)** the reasons why the financial sector is especially vulnerable to cybercrime and **(B)** the impact of cyberattacks on the financial sector.

A. Financial Sector Vulnerabilities

Rapid ICT advances have not only allowed financial sector entities to improve their performance and diversify their offerings, but have also enabled criminal networks to carry out new and increased criminal activities in the online environment. As a result, the financial services sector has become particularly dependent, and, correspondingly, susceptible to cybercrime. According to the PricewaterhouseCoopers' 2014 Global Economic Crime Survey (GECS), thirty-nine percent of financial sector respondents said they have been victims of cybercrime, compared to only seventeen percent in other industries.[89] While in the past, a person was needed to physically act to authorize and initiate fund transfers, increased reliance on ICT creates potential weak points for cybercriminals to exploit through hacking technology (*see* section 2 B, box 2.2, above).[90] Partly in light of such potentials, financial sector cybercrime appears to be on the increase.[91]

There are many reasons why financial institutions are targeted by cybercriminals, but, to use a line attributed to one infamous bank robber, mostly "because that's where the money is".[92] There are various forms of "money": banks have money in liquid form, credit card companies have it in plastic form and retailers have it derived from credit card information shared with them by consumers.[93] ICT innovations allow customers to access to their finances at any time and from any place.[94] As mentioned earlier, in December 2013, the US retailer Target was the object of a malware attack that resulted in the theft of personal information of over seventy million customers (*see* section 2 B, box 2.2, above).[95] Reports show that, each year, financial details of millions are stolen from systems operated by hotels, retail chains, banks and community service providers.[96]

Box 2.5: Vulnerabilities in Business Practice beyond Banking[97]

Business email compromise (BEC) is an exceptionally pervasive and injurious type of cybercrime. BEC commonly manifests in one of three forms: hacking of employee emails, hacking of high-level executives or exploitation of supplier relationships. BEC is a method by which cybercriminals gain the confidence of employees, employers or businesses through carefully crafted communications that imitates standard operating procedures, masquerading as legitimate. Once email account relationships are infiltrated, information needed to imitate communications is taken, thereby enabling the sending of fraudulent transaction requests. Businesses of all sizes and varieties are targeted using BEC scams, with the amount of funds stolen depending upon what is typical for that business's transactions.

Statistics compiled by the Internet Crime Complaint Center (IC3), a partner of the FBI, indicate that, between October 2013 and December 2014, there were 2126 cases of BEC amounting to a combined financial loss of US$214,972,503.30. However, as only 45 countries outside the United States sent complaints to IC3, these figures probably underrepresent BEC's global impact.

As is true of cybercrime at large, BEC scams can be launched from any country and can target any entity or individual relying upon email communications. The money trail can be as difficult to follow as the origin of the attack, as funds are frequently transferred multiple times across several jurisdictions. The nature of this particular type of cybercrime, the number of attacks and the potentially small amounts taken together make it exceedingly difficult to trace, prosecute and recover assets of such crimes.

Although cyberattacks may be carried out through malware, phishing or direct hacks, the most common method is through DDoS attacks,[98] which aim to cripple the functions of ICT systems of targeted business by bombarding their websites with requests until they are unable to cope and cease to function properly. For instance, in what has been called the "Operation Payback" campaign, the Anonymous group of hackers targeted firms seen as being anti-WikiLeaks, including MasterCard and Visa after they withdrew their services from WikiLeaks, using DDoS attacks to disrupt their web services.[99]

Although virtual currencies such as Bitcoin are still developing, their implications for financial crime are significant. Criminal networks have shown great interest in virtual currencies for the ability to carry out large-scale money laundering.[100] In addition, just as with traditional currencies, virtual currencies are susceptible to cybercrime attacks such as fraud.[101]

Various approaches have been taken to address financial cybercrime. In the United States, laws combatting wire fraud have been expanded to prosecute cybercrime. Under the US Wire Fraud Statute,the prosecution must show:

1. A scheme to defraud by means of false pretense;
2. Willful and knowing participation with intent to defraud; and
3. Use of interstate wire communications in furtherance of the scheme.[102]

Because computer transmissions are conducted by wire, the Statute remains an effective tool to fight a wide range of financial cybercrimes.

B. The Impact of Cyberattacks on the Financial Sector

According to the Center for Strategic and International Studies report,[103] the estimated annual cost of cybercrime is between US$375 billion and US$575 billion in losses, primarily borne by the private sector. This amount represents the total sum of opportunity costs, confidential business information and market manipulation, and recovery costs for the targeted institutions.[104] However, there are also substantial indirect costs associated with the theft and abuse of financial and personal information that are kept by financial institutions.

Case 2.6: United States v. Drinkman (USA)[105]

The US DoJ indicted Defendants for hacking, wire fraud and unauthorized computer access of financial institutions with the intention of stealing usernames, personal data and credit card information.[106] On 28 June 2012, Defendants, four Russians and one Ukrainian, were arrested in the Netherlands. Targeted companies included NASDAQ, 7-Eleven, Carrefour, JCP, Hannaford, Heartland, Wet Seal, Commidea, Dexia, JetBlue, Dow Jones, Euronet, Visa Jordan, Global Payment, Diners Singapore and Ingenicard.[107]

The methods of hacking utilized by Defendants included SQLi attacks, SQLi strings, malware and tunneling. All of these mechanisms were used to gain access to computer systems of the corporate victims and to extract customers' credit card data and personal information either for direct criminal gang use or for sale on the black market. This scheme mainly targeted retailers, credit card companies and other businesses by successfully invading their computer systems that process payment services.[108]

Between 2005 and 2012, Defendants retrieved information on 160 million credit card numbers as well as other personal identification information. The information thefts allegedly cost three of the targeted institutions a collective US$300 million in losses, both in direct costs from the stolen date and in subsequent remediation. The costs are under-representative, however, as the effects were not limited to retailers and financial institutions, but also extended to consumers.[109]

Cyberattacks on financial institutions are of particular concern because they undermine not only individual reputations but also consumer confidence both in that entity's online services, and in the security of the larger financial sector's offering of cyber-based services. Undermining consumer confidence decreases financial activity and, if business is shifted to more traditional means, often results in increased costs. More dramatically, it results in consumers removing their money from the financial system and placing it under the proverbial mattress, thereby further hurting the global financial system and markets. As an alternative, as indicated by Target consumers following that cyberattack, customers may, where possible, switch to making cash transactions, which also limits the efficacy and size of the market.[110]

Left unaddressed, cyberattacks targeting the personal information kept by financial institutions could have cripplingly severe impact upon economies. These costs go well beyond the immediate financial institutions that hackers target, extending to the clients of those services and having subsequent direct (lack of liquidity, opportunity costs, etc.) and indirect effects (lowered credit scores, loss of system confidence, lowered investment rates, etc.).

Case 2.7: United States v. Ulbricht ("Silk Road") (USA)[111]

Defendant, Ross Ulbricht, was convicted and sentenced to life in prison without the possibility of parole for conspiracy and money laundering charges stemming from his supposed role as "Dread Pirate Roberts", the operator of the online marketplace "Silk Road". Through anonymous payments in bitcoin, the Silk Road enabled the sale of, among other things, controlled substances, pirated software, and fake IDs.[112] Run through the Tor network, Silk Road operated on the Dark Web, a virtual space inaccessible without specialized software or access authorization.[113]

Bitcoin is a digital currency manifestation of "blockchain" technology, a method of recording data that allows for independent recording and verification of "blocks" of digital records that have been lumped together, and then cryptographically (through a technique known as "hashing") and chronologically bound in a "chain" using complex mathematical algorithms. The recording system can be generically described as a distributed database or "public ledger"; however, this ledger, to which everyone in the network has access, is not stored in any one place but rather distributed across multiple computers around the world. The only recorded data is the fact a transaction's occurrence and associated hash.[114] Not all blockchains are anonymous, and bitcoin is but one manifestation of blockchain technology.[115] Blockchain technology has been described as the most disruptive technology since the internet.[116]

Bitcoin transactions, because they are highly secure and highly anonymous, pose certain challenges to "traditional" forms of combatting financial crimes, particularly with regard to the finding and extraditing of perpetrators. However, even with bitcoin, anonymity is not complete: first, as perpetrators must "cash out" of bitcoin to realize their profits, and, second, as bitcoin's shared ledger makes transactions public, even if unidentified.

Bitcoin also raises regulatory concerns. While banking is a regulated sector, bitcoin transactions are not considered part of the banking system in many jurisdictions, often making it unclear whether banking law or cybercrime law should apply. In banking, various suspicious activity reporting (SAR) rules require financial institutions to report suspicious transactions, many, if not all, of which may not apply to bitcoin transactions.[117] That said, the inherent forensic element of bitcoin often lends itself to facilitating investigations once matters reach that stage.

VIII. Misuse of Devices

The offense of misuse of devices prohibits the use of a device, password or access code in the furtherance of the afore-enumerated acts.[118] Acts criminalizing such offenses have existed for some time and have typically been used as a means of targeted hacking by targeting the tools enabling

cybercrime.[119] Password trafficking is the sharing or trading accounts—often after passwords have been stolen through hacking techniques—with potential for immediate financial reward or access to private information.[120] Such behavior is criminalized for all of the reasons discussed above, but notably because it diminishes the security and reliability of computer data and of cyberspace as a whole. An example of this crime is computer-related forgery.[121] The offense can be difficult to ring-fence, however.[122]

As ready-to-exploit kits are becoming widely available, creating, possessing or distributing hacking software or tools for committing cybercrime must be criminalized.[123] Moreover, much technology developed for legitimate purposes has been coopted in order to facilitate cybercrime.[124] Keeping these dual use devices away from only cybercriminals presents certain legal obstacles.

Case 2.8: Geoffrey Andare v. Attorney General (Kenya)[125]

In April of 2015, Andare was arrested for violating a Kenyan law criminalizing the misuse of ICT subsequent to his having posted a message on his social media page reprimanding an agency official for allegedly exploiting others. Section 29 of the Kenya Information and Communications Act—"the improper use of an ICT system"—criminalizes the use of any licensed telecommunication system, such as a mobile phone or computer, to "send[] a message or other matter that is grossly offensive or of an indecent, obscene or menacing character".[126] It also imposed a penalty of a fine not exceeding KSh50,000, or imprisonment for a term not exceeding three months, or both.[127]

In April of 2016, High Court Judge Mumbi Ngugi struck down that section of the law as violating the constitutional right to freedom of expression,[128] and also as being overly broad and suffering from vagueness.[129] The law, it was determined, had a chilling effect on legitimate online expression. In reaching her decision, the judge offered that the laws of Libel are sufficiently robust, referring to a recent case where damages of KSh5 million were awarded against a blogger for defamation by a separate court which relied on laws of libel.

Conclusion

This section has discussed certain core and evolving cybercrime acts—namely, hacking, unauthorized monitoring, data alteration, system interference, computer content-related offences, cyberstalking, financial cybercrimes, ransomware, misuse of devices and intellectual property infringements (including cybersquatting). Even with regard to these universally-frowned upon activities, there is not universal consensus that these activities should be criminalized, and, where

there is consensus, no consensus on how or to what extent. Such is particularly true of content-related offences. To amplify the capacity-building purposes of the Toolkit, however, a broad net is cast.

As there is consensus on the appropriate delineation or categorization of cybercrimes—especially where they have substantial "offline" activities—, it is often difficult to determine which legislative provisions should govern ICT-related criminal conduct. Moreover, even in instances where the behavior is considered both undesirable and illegal, it is not always clear that cyber law is the appropriate governing law, as the Silk Road case shows.[130] Those difficulties are further exacerbated on the international stage, especially when trying to create cooperation among law enforcement agencies.

C. Procedural Issues

Table of Contents

Introduction

Information security issues are global in nature. However, while cybercrime is transnational, the means of investigating and prosecuting crimes is territorially defined, and often defined quite locally at that. In addition to tools and training, investigators require appropriate investigative powers and procedural instruments in order to identify offenders and collect evidence. While these measures may not necessarily be cyber-specific, the possibility of offenders acting remotely from the locus of the victim means that cybercrime investigations are very frequently conducted differently from traditional ones.

In looking at the procedural issues[1] surrounding the search and seizure of in cyberspace, this section considers how to **(I)** adapt traditional search and seizure techniques to the digital world, **(II)** the role that third parties play in evidence collection and **(III)** the implications of technological developments, notably that of cloud computing, for evidence collection and in creating jurisdictional conflicts.

I. Adapting Search & Seizure to the Digital World

In cybercrime, just as in traditional crimes, crucial incriminating evidence is often found during search and seizure operations. Existing search and seizure procedures can be **(A)** adapted to cybercrime searches and seizures, but must also be **(B)** limited according to the principles of relevance and effectiveness, which **(C)** states have done in varying ways. However, while technological developments have made more work for investigators, **(D)** advanced forensic tools can be used as means of identifying relevant e-evidence.

A. The Challenges of Adapting Existing Procedures

"The devil", it is said, "is in the detail". While reaching consensus on issues of substantive law is a complicated matter, difficulties multiply when discussions turn to procedural law: while the purpose of substantive law is to define the extent of rights and duties, the purpose of procedural law is to regulate the proceedings providing access to those substantive rights and responsibilities. Thus, although there may be agreement on the underlying right, defining how that right is accessed, and what precludes it, requires a greater degree of accord.[2] Moreover, the ever-evolving nature of cybercrime requires that procedural law, just as with substantive law, keep pace with new abuses and new technologies.[3]

The challenge is setting regulation that permits rapid transactions around the world but which relies upon local legal and investigative instruments. Moreover, the swift pace of technological development and the difficulties this poses for designing, updating and disseminating effective technical security measures complicate procedural matters in a way that is not necessarily problematic for substantive law. As discussed further on, arrangements at the international level might overcome many of these procedural barriers where a formal consensus or an informal working arraignment can be found (*see* sections 3 A and 3 B, below). In the short-to-medium term, cybercrime countermeasures will need to build upon, or at least take into account, existing national and regional efforts to combat cybercrime and terrorism.[4]

B. Delimiting Searching & Seizing e-Evidence

Search and seizure procedures play a critical role in securing evidence necessary to proving culpability. An active mode of investigation, search and seizure involves discovering evidence, identifying suspects, apprehending offenders and interviewing witnesses. Investigating cybercrime requires different techniques, not only because of the cross-jurisdictional nature of cybercrime (*see* section 1 B, above),[5] but also due to the very nature of cyberspace and of e-evidence (*see* section 2 D, below).[6]

The traditional search-and-seizure approach focuses on collecting and cataloging physical material. Due to rapid developments in cyberspace, however, most evidence, though stored on physical devices, exists only in a digital format. Legal authority and good practices for executing search and seizure warrants varies considerably between jurisdictions and criminal justice systems, especially with regard to rules governing handling e-evidence.[7] As such, it is incumbent upon investigators to consider the appropriateness of previewing and forensically acquiring data at the scene and whether the circumstances may justify physically seizing equipment for further analysis in a laboratory.[8] Retrieving such information requires augmented investigatory approaches, as well as different evidence-handling techniques.[9]

The first major procedural issue in pursuing cybercrimes is legislative: procedural law must be changed or adapted to authorize investigators to search and seize computer information, and not only tangible evidence.[10] This process presents its own complications. For example, while the United States first drafted procedural laws for authorities to access electronic communications in 1986, law makers at the time only had the telephone in mind, and, accordingly, drafted a limited law specifying that it applied to telephone-related crimes.[11] The law soon became outdated and had to be amended to include other existing and anticipated forms of electronic communication; however, that process of revision caused delay and hindrances, and was only done following the terrorist attacks of 11 September 2001.[12] Computer information, or data,[13] is information that is either stored in a storage device, or which is in transit across virtual networks (*see* section 2 A, above). First responders investigating cybercrime frequently seize all relevant devices.[14] However, as the storage capacity of ICT devices has grown—and continues to grow—exponentially,[15] and as the nature of digital documents continues to diversify, much of the information stored on any given device is ordinary business material or private information lacking any investigatory relevance. This trend[16] is exacerbated by increasing device capacities[17] and the falling costs of digital as opposed to physical storage.[18]

The principles of relevance and effectiveness are of great importance for the admissibility of e-evidence.[19] Indiscriminate or arbitrary search and seizure techniques risk being excessively intrusive. Since the data is not the device itself, and since much of the information on the device is not relevant to the investigation, the device itself should not be seized unless the warrant describes, with particularity, that such is what agents should search for and seize.[20] Otherwise, computer hardware should only be seized if it itself is contraband, evidence, fruit or an instrumentality of crime.[21] If, by contrast, the probable cause relates only to information, then the warrant should describe the information to be seized, and then request the authority to seize the information in whatever form it may be stored (electronic or otherwise).[22] Agents seizing hardware should explain clearly in the supporting affidavit that they intend to search the computer for evidence and/or contraband after seizure and removal from the site of the search.[23] Indeed, indiscriminately seizing devices would be the equivalent of entering an investigation scene and seizing everything without any consideration of what was being seized. By contrast, even if the warrant does not describe hardware itself, identification of a device's IP address and separate email address linked to same physical location, for instance, may be sufficient to justify hardware seizure.[24]

Case 2.9: Korean Teachers & Education Workers' Union (2009Mo1190) (Korea)[25]

Korean investigators executed a warrant of search and seizure upon the headquarters of the Korean Teachers & Education Workers' Union, removing ICT devices containing huge amounts of digital information back to their police offices, where they made copies of the files for subsequent search and analysis. The Court held that the action was allowed, as the quantity of data—over 8,000 files—to exceptional circumstances justifying such removal, even though there was no explicit ground under the warrant for doing so, and as investigators made an effort to "to limit the scope of their investigation to those parts bearing relevance to the charged crimes by copying only those files which had been accessed after a retroactively determined point of time", with the parties implicitly agreeing on the appropriateness of such measures.[26]

The Court held that, "[i]n principle, a warrant of search and seizure for digital information must be executed by collecting only parts related to the suspected facts for which the warrant has been issued[….] In cases where circumstances on the site where the warrant is to be executed make it impossible or remarkably difficult to carry out the warrant in this manner, exceptions can be made to allow the storage media itself to be carried off-site […] when the warrant expressly grants for search and seizure to be performed in this manner and when such circumstances exist."[27] The Court continued that the subsequent searching and analyzing of digital information must be "must also be seen as a part of executing the warrant".[28] Moreover, where investigators seize ICT devices containing private information extending beyond information pertaining to the suspected facts, the parties "are continuously guaranteed the right of participation in the process" and not only must "no viewing or copying of the storage media is performed without [their] involvement", but investigators must assure that "proper measures are taken to prevent files or documents from arbitrary copying or from distortion, misuse or abuse of the digital information".[29]

In effect, the ballooning of an individual's digital footprints may mean that the data—not the devices—should be screened and searched. While there may be certain circumstances where the device itself may be seized—for instance, in order to restore deleted data, to recover encrypted data, or to conduct detailed analyses—, in principle, the relevant data should be extracted from the storage device, and the device itself left on site. Many field tools are currently available to assist on-site data extraction.[30] As discussed further on, tools alone are insufficient: on-site data extraction requires sophisticated technical competency and training. Without such capacity, first responders may find themselves faced with the impossible decision of either seizing the suspect hardware and risking exceeding the scope of the search warrant, therein both infringing fundamental rights and risking "tainting" the seized evidence, or leaving the hardware and risking letting evidence

be lost or destroyed. Prior to commencing a search, investigators should ensure that they abide by applicable laws or risk having seized exhibits declared inadmissible at trial.[31] Identifying and selecting relevant hardware has become a major part of an investigation.[32]

Indeed, while the proverbial "smoking gun" might be found in a subsequent review of seized information, that information may be excluded as illegally obtained evidence.[33] In the context of electronic information, illegally obtained information is usually information that was obtained by seizing more than what was specified in the warrant—for instance, if the warrant specifies data and the device was (also) seized. Thus, while investigators may rely on a subsequent review of the collected evidence, the threat of exclusion of that information as evidence operates as a check on investigatory abuse.[34]

C. Examples of Good Practice

A considerable number of countries have prescribed—through legislation, regulation or court decisions—the scope of searches of digital information.

In the United States, the courts have crafted procedures that differentiate between searching device and data, and which require explicitness in the warrant, and that the default is a two-stage search process. The US Federal Rules of Criminal Procedure—drafted, issued and approved by the federal judiciary[35]—note the nuance between device and data stored on that device, stipulating that a warrant must say whether it is authorizing "the seizure of electronic storage media or the seizure or copying of electronically stored information".[36] The Rule continues by saying that, "[u]nless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant" and that "[t]he time for executing the warrant […] refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review".[37] The notes to the Rules prepared by the Advisory Committee make it clear that, unless the warrant explicitly specifies otherwise, the initial search done at the time of seizure need not be more than cursory, with evidentiary reliance being placed on the subsequent review of the seized or copied materials.

That position has been reiterated and followed by the courts:

> "Computers and other electronic storage media commonly contain such large amounts of information that it is often impractical for law enforcement to review all of the information during execution of the warrant at the search location. This rule acknowledges the need for a two-step process: officers may seize or copy the entire stage medium and review it later to determine what electronically stored information falls within the scope of the warrant."[38]

The Supreme Court of the Republic of Korea has taken a similar position to that of the United States, stating that:

> "In principle, illegally obtained evidence is not admissible and accordingly, such evidence cannot be used as an evidence to prove guilt of the criminal defendant."

The Court went on to say:

> "In order to render a final determination of admissibility of illegally obtained seized item, comprehensive consideration should be given to the issue of whether or not violation made by investigative agencies impedes substantial contents of due process by taking into account following factors including 1) the substances and degrees of investigative agency's violations, 2) the intention of investigative agency, 3) natures and the extent of the infringement of rights or legal interests protected by procedure rules, and so on."

Case 2.10: Customs Evasions Case (Korea)[39]

Korean law enforcement agents searched the offices of Company A on suspicion of tariff evasion by lowering unit cost for importation, seizing documents and electronic data. In the process for the search and seizure, documents and electronic data pertaining to Company B—not specified in the warrant—were also seized. On the basis of the seized information, Company B was subsequently charged after it was confirmed that Company B had evaded tariffs in the same manner as Company A based.

The Supreme Court of Korea subsequently excluded the evidence on the basis that, first, the evidence was not collected in accordance with the procedures as set forth in the Constitution and Criminal Procedure Act, and, second, the secondary evidence failed to follow legal procedures for the protection of fundamental human rights: in principle, the Court ruled, secondary evidence cannot be admitted as evidence to prove guilt. The Court provided that "[d]ocuments and electronic data relating to Company B which were seized, along with seizure of those pertaining to Company A, were neither the object to be seized as stipulated by a search and seizure warrant nor related to the facts of suspicion."

The Court further censured the investigators lack of discrimination between data and device, noting that "[a]fter moving the storage device itself into the office of the investigative agency, and then investigating the electronic information related to facts of suspicion, either the process of printing the concerned electronic information into documents or the process of

copying the files included in the execution of a search and seizure warrant. In this case, the object of the document-printing process or file-copying process should be confined to the part related to facts of suspicion as specified in the warrant."

By contrast, some countries have cited the successful extension of general search and seizures powers. South African representatives, for example, reported favorably on the nation's Criminal Procedure Act, which, though not specifically making provision for the seizure of e-evidence, allowed authorities to seize "anything".[40] Other countries also reported that it was good practice for investigative powers relating to computers and other devices to "extend to all crimes and not just traditional computer crimes", and that relevant procedural laws should be both "comprehensive" and "precise".[41] While such general extensions of power may be warranted and possibly even advisable, it bears noting that judicial oversight to disallow evidence obtained as a result of overly-broad search under more general principles should still be assured and authorized.

D. Techniques for Identifying Relevant e-Evidence

An analysis of available hardware components can, for example, prove that the suspect's computer was capable of carrying out a DDoS attack or is equipped with a chip that prevents manipulations of the operating system. Hardware analysis can also be necessary in the process of identifying a suspect. However, hardware analysis does not always mean focusing on physical components attached to a computer system. Most operating systems keep logs of hardware that was attached to a computer system during an operation.[42] Based on the entries in log files such as the Windows Registry, forensic examiners can even identify hardware that was used in the past but was not present during the search and seizure procedure.

In addition to hardware analysis, software analysis is a regular task in cybercrime investigations. Software tools can be installed to match the functioning of computer systems to the demand of the user. Forensic experts can analyze the functioning of software tools in order to prove that a suspect was capable of committing a specific crime. An inventory of software tools installed on the suspect's computer can also help to design further investigation strategies. If, for example, the investigators find encryption software or tools used to delete files securely, they can specifically search for encrypted or deleted evidence.[43] Investigators can also determine the functions of computer viruses or other forms of malicious software and reconstruct software-operation processes.[44] In some cases, where illegal content has been found on suspects' computers, the suspects have claimed that they did not download the files but that it must have been done by computer virus. In such cases, forensic investigations can try to identify malicious software installed on the computer system and determine its functions. Similar investigations can be carried out if a computer system could have been infected and turned into part of a botnet.[45]

Software analysis can also be important to determine if software is produced solely for committing crimes or can be used for legitimate as well as illegal purposes (dual use). This differentiation can be relevant, insofar as some countries limit criminalization of the production of illegal devices to those that are either solely or primarily designed to commit crimes. Data-related investigations are not confined to the software function, but also include analysis of non-executable files such as pdf-documents or video files. File analysis also includes the examination of digital documents that might have been forged[46] as well as metadata investigation.[47] Such analysis can determine the time[48] the document was last opened or modified.[49] Furthermore, metadata analysis can be used to identify the author of a file containing a threatening message, or the serial number of the camera that was used to produce a child-pornography image. Authors can also be identified based on linguistic analysis, which can assist in determining if the suspect has written articles before and left information that can help identification in this context.[50]

As investigators must focus on relevant evidence in order to prevent inadmissibility, special attention must be given to identifying relevant evidence,[51] meaning that forensic experts play an important role in the design of investigation strategies and the selection of relevant evidence. They can, for example, determine the location of relevant evidence on large storage systems. This enables investigators to limit the scope of the investigation to those parts of the computer infrastructure that are relevant for the investigation and avoid inappropriate and large-scale seizure of computer hardware.[52] This selection process is relevant as various types of storage devices are available that can make identification of the storage location of relevant evidence challenging.[53] This is especially valid if the suspect is not storing information locally but uses means of remote storage. Forensic analysis can then be used to determine if remote-storage services were used.[54]

Identification of relevant digital information is not confined to files themselves. Databases of software tools that are made available by operating systems to quickly identify files might contain relevant information too. Another example of evidence identification is the involvement of forensic experts in determining the right procedural instruments. A number of countries enable law-enforcement agencies to carry out two types of real-time observations—the collection of traffic data in real time, and the interception of content data in real time. In general, the interception of content data is more intrusive than the collection of traffic data. Forensic experts can determine whether the collection of traffic data is sufficient to prove the committing of a crime, and thereby help investigators to strike the right balance between the need to collect effective evidence and the obligation to protect the rights of the suspect by choosing the least intensive instrument out of the group of equally effect options. Both examples show that the role of forensic investigators is not restricted to the technical aspects of an investigation, but includes a responsibility for protecting the suspect's fundamental rights and thereby avoiding inadmissibility of the evidence collected.

II. Collecting Evidence with the Assistance of Third Parties

To obtain cybercrime evidence, collaborating with third parties, such as ISPs,[55] is vital, as considerable amounts of evidence of cybercriminal activity are stored in information systems managed by third parties. In order to prevent law enforcement from overstepping its powers in such data acquisition, it is important to clearly define what type of information might be acquired, as well as the procedures for requesting and, if necessary, compelling third parties to release that information. Various factors—including where the ISPs are located (both their servers and other hardware), available legal mechanisms and terms and conditions of user agreement—will determine the tone of the third-party cooperation.[56] As significant human rights considerations surround such activities, especially around the freedom of communication, it is incumbent upon both law makers and authorities to implement laws and regulations appropriately balancing government power with individual rights. These matters are discussed in greater depth below (*see* section 4 A, and 4 B below).

It is important to realize that not all data is the same, and, as such, that there may be varying degrees of potential privacy considerations, for example. It is also important to distinguish between areas where voluntary cooperation may be appropriate as opposed to situations where third parties are compelled to cooperate with law enforcement. Both are discussed below.

Three different classes of stored communication should be differentiated:

1. Subscriber information;
2. Communication records or logs; and
3. Communication content.

Subscriber information is relatively basic, pertaining to identifying information such as the subscriber's name, contact and payment details. Such information is typically needed by investigative authorities in order to make requests to obtain warrants and other public requests.

Attaining subscriber information—the first type of data—typically implicates fewer privacy concerns than does seeking access to the content of communications, and, as such, this information is generally subject to fewer safeguards and limitations. To facilitate investigations while also protecting individual privacy, laws should further distinguish between basic customer information and information detailing account activity.

The second class of data, communication records or logs, are more detailed, and includes IP address(es) of device(s) used by person(s) under investigation, time of transmitting and receiving electric communications, data volume, communication ports, protocol information and the like. As acquiring this information is a significantly greater infringement of privacy, the law should clearly define and delineate both the scope of communication records that might be acquired and the procedures for doing so. Typically, court orders are issued on the basis of "reasonable grounds" showing that the communication record is relevant to the investigation in progress. Moreover, these laws frequently require that, upon completion of the investigation or the prosecution, the investigative agency notify the investigated party of the data acquisition. That said, in some

countries, notification must be made prior to data acquisition if the communication record is collected through a court order rather than through a search and seizure warrant.

As communication content, the final type of third-party stored communication, is the most sensitive form of communications, a search and seizure warrant is invariably required, meaning that the request must make a showing that the desired information is necessary to clarify the "probable cause" relating the object of the search and crime. Here, the procedural law should consider whether all categories of stored content deserve the same kinds of protection. For example, there is a lower expectation of privacy for information in cloud storage as opposed to the contents of an email. Therefore, a full search warrant may be appropriate for emails, whereas only a grand jury subpoena or a court order may be appropriate for cloud-stored information.

Cooperation with the private sector, discussed further on, is an essential element to combatting cybercrime (*see* section 6 C, below). With respect to the present discussion, it bears noting that ISPs, in particular, potentially play an especially important role in many cybercrime investigation as, in many cases they have the technical capability to detect and prevent crimes to support law-enforcement agencies. That assistance is especially relevant in connection with identifying suspects. Obligations discussed range from the mandatory implementation of prevention technology to voluntary support of investigations.[57] Cooperation between law-enforcement agencies and ISPs requires the application of certain procedures.[58]

One example is the forensic tool CIPAV (Computer and Internet Protocol Address Verifier), which was used in the United States to identify a suspect who had been using anonymous communication services.[59] Another example of cooperation between ISPs and investigators is email investigation. Emails have become a very popular means of communication.[60] To avoid identification, offenders sometimes use free email addresses which they were able to register using fake personal information. However, even in this case, examination of header information[61] and log-files of the email provider will in some instances enable identification of the suspect.

The need to cooperate and communicate with providers is not limited to ISPs. Since some crimes such as phishing[62] and the commercial distribution of child pornography include financial transactions, one strategy to identify the offender is to obtain data from financial institutions involved in the transactions.[63] In Germany, for example, investigators worked with credit-card companies to analyze and identify customers who had purchased child pornography on a specific website.[64] Such investigations are more challenging when anonymous payment methods are used,[65] such as bitcoin.[66]

Law enforcement often require third-parties to provide communications in real-time. Such is particularly true where there are indications of imminent perpetration or harm, especially in cases of terrorism, and where real-time collection may offer critical evidence. Furthermore, some information can only be captured in real-time as it is never stored (instead existing only in the "cloud"). The communication record (the second class of information) can be had in real-time by monitoring current IP addresses of transmitters and receivers, thereby helping to geolocate suspects. Such

information might also be helpful in figuring out party relationships in crimes in progress. More dramatically, real-time communication content (the third class of information) can be intercepted with the assistance of third parties. Because of the sensitive nature of both the information, and the manner in which it is being acquired, the law should specify not only the appropriate requirements and procedures for such requests by law enforcement, but also which offenses are subject to interception. Typically, a court's approval is required, with the requirements for an interception warrant being stricter than those for a seizure warrant. Due to the sensitivity of such requests, numerous cases where it is impossible to secure communications data, even where there are legitimate reasons, exist.[67]

Lastly, law enforcement may also require the assistance of third parties in preserving data. Information stored by service providers can easily disappear: intentional deletion by subscribers, withdrawal of services by subscribers or automatic deletion policy of service providers are but a few of the ways in which this information can disappear. In order to prevent such evidence loss, measures for preserving data after detecting a link between the data and crimes must be put in place. Data preservation is based on the initiation of a compulsory procedure, therein allowing investigators to obtain the desired data.

III. Cloud Computing

Cloud computing is the use of a network of remote servers hosted on the internet rather than a local server or a personal computer to store, manage and process data. Evolving cyberspace technologies—especially cloud computing—result in both **(A)** technological complications to search and seizures, as well as more serious **(B)** jurisdictional complications.

A. Technological Complications to Search & Seizures

Due to the flexibility that cloud computing offers users to rent data storage, software and network broadband for services ranging from web-mail to data storage, the practice has become increasingly common. Cloud computing is yet another example of how ever-changing cyberspace capabilities and usages require the legal framework to change and adapt—in this case moving away from the traditional, and now no longer relevant, concept "of the place to be seized". In cloud computing environments, data subject to search and seizure can be expanded to include information stored in a remote location by a cloud computing service provider.

Cloud computing also allows for so-called "virtualization" technology. Virtualization creates virtual computing resources by combining various resources of computers physically existing in different physical locations. Using this technique, data stored by cloud-computing users appears to be stored in a virtualized storage device.

Distributed databases, by which data is copied, maintained and distributed across servers in various locations, therein offering greater safety and security, complicate localization of data. Through the use of a centralized distributed database management system (DDBMS), the data is synchronized and integrated logically, allowing the user to manage it as if it were all stored in the same location. Distributed databases can be either homogenous or heterogeneous. In a homogenous system, all of the physical locations have the same underlying hardware and run the same operating systems and database applications, while in a heterogeneous system, the hardware, operating systems or database applications may vary at each of the locations. Together with the use of a technique known as "sharding"—a type of database partitioning by which large databases are separated into smaller, more manageable parts called data shards—, accessing comprehensible information can be quite challenging, both for law enforcement and for hackers. Mutual legal assistance treaties (MLATs) facilitate extra-jurisdictional requests for data (*see* section 3 A, below), and can be particularly useful in these circumstances.[68] Where a service provider utilizes a foreign cloud data center (*e.g.*, Amazon Web Services), the data frequently resides in a country other than where the service provider is registered.

Notwithstanding the fact that data might be fragmented and stored in several servers, and identical copies may co-exist simultaneously in different places, it is often possible to retrieve that data intact by relying on service providers' control of the cloud service mechanism. As such, in a spin on traditional understanding, the user's account together with the name and the headquarter address of the cloud service provider is designated as the "place" subjected to search and seizure rather than a physical location. The US DoJ has provided examples of how a search and seizure warrant against an email account might be prepared.[69] Consequently, the execution of a search and seizure warrant in cloud computing environments depends on service providers that control the locations and methods for data storage. The execution of a search and seizure warrant in cloud computing environments is conducted by when law enforcement present the warrant to service providers. Execution of a search and seizure warrant in cloud computing environments can be compared to general forms of search and seizure that require direct participation of investigative authorities.

An account in the cloud subjected to search and seizure may be designated differently depending on the internet source used by the offenders: for instance, if webmail is used, the mail account is designated as the one to be seized; when a web drive is used, the URL address is designated for seizure; if web hosting servers are being used, then those IP addresses are selected for seizure.

B. Jurisdictional Complications to Search & Seizures

While developing technology complicates procedural aspects of search and seizure, more fundamental issues arise over jurisdictional conflicts. Although the question of jurisdiction is discussed in greater depth hereafter (*see* section 2 E, below), it bears raising the topics here specifically with regard to procedural matters. Cloud computing has particularly complicated

matters from a jurisdictional standpoint, as many cloud service providers have centers around the world; as a result, jurisdictional disputes between the country where cloud service providers are registered and those where data is stored is growing. Moreover, as discussed, data is frequently fragmented, with parts and pieces not only in various places but in various countries. Once these logistical, storage issues are coupled with issues of data privacy (*see* section 5 B, below), these jurisdictional conflicts can cause intense disputes.

Case 2.11: Microsoft Corp. v. United States ("Microsoft Ireland") (USA)[70]

In connection with the provision of its email and cloud-based services, Microsoft required its subscribers to provide certain location information when requesting email and other services. That information was stored in data centers proximate to the location identified by the subscriber. Much of the metadata related to such subscribers (with the exception of certain communication content data) was stored in the United States.

In December 2013, the US District Court for the Southern District of New York issued a search warrant on Microsoft authorizing US law enforcement authorities investigating drug trafficking operations to obtain communication data of users that had their data stored in datacenters outside the United States. Microsoft entered a motion to quash the warrant, claiming that the communication content of the concerned email accounts was stored in a data center located in Ireland, arguing that such communication content is beyond the scope of the warrant.

On 25 April 2014, the US Magistrate Judge issued an order denying Microsoft's motion to vacate the warrant, holding that "an ISP located in the United States would be obligated to respond to a warrant issued pursuant to Section 2703(a) [of the US Stored Communications Act (SCA)[71]] by producing information within its control, regardless of where that information was stored."[72] On 31 July 2014, the US District Court for the Southern District of New York affirmed the Magistrate's Order.[73] Microsoft appealed to the US Court of Appeals for the Second Circuit.

The case quickly became a hotly contested one. Private sector entities (including AT&T, Apple and Cisco) raised concerns that the warrant would have to their business environments in amicus curiae briefs; and digital rights groups said it would have been an unwarranted intrusion.

On 14 July 2016, a three judge appellate panel ruled in favor of Microsoft, concluding that Congress did not intend that a warrant issued under the SCA to have any extra-territorial effect. The Government has petitioned for a rehearing *en banc*.

Conclusion

Traditional search and seizure procedures focus on the collection of physical evidence. However, e-evidence has different properties, requiring different search and seizure approaches, which must be dictated by the legal framework. Careful attention must be paid to creating procedures that accommodate the difference between digital information and digital storage devices, and which respect fundamental rights, notably the right to privacy, by limiting the scope of the search and seizure, as prescribed by the warrant. In many jurisdictions, judicial bodies have been attentive to excluding information as evidence of guilt where it has been illegally gathered as beyond the scope of the warrant.

Third parties are often essential to the collection of evidence. In order to collect communication data managed by third party (*e.g.*, subscriber information, communication records, communication content), and to do so in real-time, appropriate procedures need to be implemented directing those parties to offer technical and administrative support to law enforcement. Moreover, ISPs not only store subscribers' data but also have their own technologies and metadata that are of value to law enforcement. Procedures obliging ISPs to cooperate with law enforcement should be based on (1) the classification of requests for data preservation; (2) the acquisition of the stored communication data; and (3) the real-time collection of communication data. Provisions guaranteeing ISPs exemptions from both civil and criminal liabilities that could arise out of third parties' provision of data should accompany such procedures. Procedures obliging ISPs to cooperate must also strike an appropriate balance between respecting fundamental rights and accounting for cyberspace's rapidly evolving nature.

Rapid technological advancements, notably cloud computing, make create an ever-evolving technological morass through which law enforcement must seek to navigate. The development of cloud computing requires also a legal development with respect to the procedures for search and seizure. Moreover, even once technological obstructions have been surmounted, jurisdictional ones often persist given the disparate physical that support the existence of cyberspace; such issues require an ever-greater push to create a shared, international consensus, if not a single vision. As discussed further on (*see* section 5, below), it is important to establish corresponding procedural safeguards to protect personal data and privacy rights, as well as to the define limits of procedural powers utilized to investigate cybercrime and to gather e-evidence.

D. Evidentiary Issues

Table of Contents

Introduction

Due to the legal tenet of the presumption of innocence—*ei incumbit probatio qui dicit, non qui negat*[1]—, the burden of proof lays with the prosecuting authorities.[2] That burden is met by proffering sufficient evidence to meet the requisite standard of proof (*e.g.,* beyond reasonable doubt; clear and convincing evidence; preponderance of the evidence). Cybercrime being governed by criminal law, the standard of proof is higher than in either administrative or civil proceedings.

Regardless of the type of case, or of the nature of the allegation in question, the case will be decided by the trier of fact based as much upon the authenticity, integrity and the reliability of the evidence as on its quality. Digital or e-evidence presents interesting

challenges. This section **(I)** explores how best to assure the authenticity, integrity and reliability of e-evidence, before turning to **(II)** understanding the "hearsay" rule as it applies to e-evidence.

I. Computer Forensics

Computer forensics is not only necessary to establishing the appropriate proceedings by which cybercrimes are investigated (*see* section 2 C, above), but also necessary to the collection of e-evidence. To enter into such a discussion, it is important to consider **(A)** the nature of e-evidence and **(B)** the nature of the corpus of law of evidence. On the basis of that understanding, **(C)** the role of computer forensics can be discussed.

A. The Nature of e-Evidence

As with so much in cyberspace and cybercrime, there is no single definition of a term "digital" or "electronic" evidence ("e-evidence"). For purposes of the Toolkit, the term will be used to refer to "information stored or transmitted in binary form that may be relied in court".[3] E-evidence is used as a proof of crime in the same way as physical evidence. Indeed, beyond "pure" cybercrimes, the development of cyber services and the widespread supply of ICT devices have led to increased use of e-evidence in prosecuting traditional, physical-world crimes.

Digital information is electronic by definition and by nature, and therefore has a "virtual" and "imaged" existence. As such, and unlike physical evidence, digital information is not "fixed" to a single device, meaning that it can be easily copied and reproduced onto another device without any alteration or loss of information. However, as courts have generally required original evidence when considering physical evidence, and only relatively rarely allow copies to be presented as evidence, the ease and completeness with which digital data might be reproduced and transposed has led to discussions about whether copies might, in fact, be presented as identical to the "original" copy. By and large, it is impractical to present anything other than the copy of the original e-evidence; indeed, as already discussed,[4] sometimes taking a copy of the original digital data is the only way that investigators can examine the often-vast array of information confronting them.

As e-evidence is effectively an electronic image constructed out of code, it is much more susceptible to alternation than most physical evidence. Both intentional and unintended alterations might occur if vigilance is not assured. As this vulnerability might lead to claims of unreliability, it is especially critical that investigators assure and preserve the authenticity, integrity and reliability of the original copy of e-evidence throughout the chain of custody, from collection, through analysis and to submission to the court.

B. The Law of Evidence

The law of evidence, a procedural body of law, governs how various forms of proof of misdoing are presented and evaluated, typically for presentation at trial.[5] It consists of rules and procedures governing the proof of a particular set of facts in issue.[6] Matters of evidence are concerned with presenting evidence supporting both the occurrence of events, and the implicated actors thereto. For the purpose of legal proceedings, the concept of electronic evidence may have specific recognition, or it may be admitted as analog evidence, such as in the form of a document, with the meaning of what constitutes a document invariably extending to anything recorded in any form, which must be right.[7]

From a legal perspective, electronic evidence needs to be:

1. **Admissible,** meaning that it conforms to legal rules;
2. **Authentic,** meaning that the evidence can be shown to be what the proponent claims it is;
3. **Complete,** meaning that it tells the whole story and not just a particular perspective;
4. **Reliable,** meaning that there is nothing about how the evidence was collected and handled that casts doubt about its authenticity and veracity; and
5. **Credible,** meaning that it is believable and understandable by a court.[8]

From a legal perspective, e-evidence can be defined not only on the basis of what it is—that is, as the legal object constituted by data expressed in electronic format, as defined above—, but also as a construct—that is, the representation of facts or acts legally relevant to the matter and conducted by electronic means. Regardless of which aspect is considered, technical and legal analysis is required in order to show how the evidence was obtained, as well as how to interpret it and show how it pertains to the criminal matter.

C. Computer Forensics

Computer forensics plays an essential role in both **(1)** investigating cybercrime and **(2)** identifying, collecting and preserving evidence.

1. Investigating Cybercrime

Investigating a cybercrime may involve invasive surveillance, as followed up by search and seizure.[9] Prior to any search and seizure, however, investigations typically begin by proving that the suspect had the ability to commit the crime. Although surveillance of suspects can reveal a great deal—for instance, establishing the requisite know-how, or observing unusually heavy volumes of data traffic to a computer that incriminates the alleged perpetrator[10]—, those initial suspicions and circumstantial evidence must be corroborated.

Regardless of the crime, traces of the perpetrator and how the crime was committed are left behind.[11] Forensics is the use of scientific tests or techniques in connection with the detection of crime.[12] Computer forensics refers to the systematic collection of data and analysis of computer technology and information with the purpose of searching for e-evidence.[13] Generally utilized after the commission of the crime,[14] computer forensics is a major part of cybercrime investigation. Indeed, its centrality to the investigation's success emphasizes the need for training and capacity-building in this area, as well as the sharing of resources and of information.[15] While forensic techniques in traditional crimes typically rely upon physical evidence—DNA, splatter patterns, chemical analysis[16]—computer forensic techniques rely upon a variety of digital sources—emails, connection logs, various metadata[17]—; each present their own unique challenges.[18]

Computer evidence comes in a variety of forms and can be found in a variety of places. Regardless of the location of that evidence—be it on a perpetrator's hard drive, in the records of a third party provider (such as an ISP) or in fragments scattered around the world (such as in cloud computing)—, procedures are required for gaining access. As already discussed, traditional search and seizure procedures already in existence must be adapted to make the accommodate the novelties of cybercrime investigations (*see* section 2 C, above). Following search and seizure, forensic experts are required to examine not only hardware and software but also the various and sundry metadata.[19]

2. Identifying, Collecting & Preserving Evidence

Collecting digital or e-evidence requires diverse and complex technical skills. For instance, techniques for accessing and retrieving evidence stored on hard drives differ drastically from those required to intercept data being transmitted.[20] Moreover, time is often of the essence, both due to the fragility of the evidence, and given the immediacy of actions taken in cyberspace, often requiring quick decision-making off of investigators. For instance, a common question is whether investigators should shut down a running computer system. There are reasons for going in either direction: for instance, shutting down the system might be necessary in order to prevent alteration of digital information and thereby preserve the integrity of relevant e-evidence.[21] That said, "pulling the plug" may actually result in the loss of other evidence, such as temporary files that require programs, applications or internet connections to be maintained and kept running or operating. However, power disruption can activate encryption,[22] thereby hindering access to stored data,[23] and, if the appropriate security is put in place, possibly even resulting in the destruction of digital information. Additionally, even after the decision has been reached, the appropriate investigative procedures must be followed.

First responders, who undertake the first steps to collect e-evidence, bear a significant responsibility for the entire investigation process, as any wrong decision can have a major impact on the ability to preserve relevant evidence.[24] If they make wrong decisions on preservation, important traces may be lost. Forensic experts need to ensure that all relevant evidence is identified.[25] Doing as much is often difficult, with various tricks employed by offenders, such as hiding files in separate storage device or scattered across the cloud in order to prevent law enforcement from finding and analyzing

their contents. Forensic investigators are essential to identifying hidden files and to making them accessible.[26]

Forensic investigators are similarly needed for recovering deleted or destroyed digital information.[27] Files that are deleted by simply placing them in a virtual trash bin—even if "emptied"—do not necessarily render them unavailable to law enforcement, as they may be recovered using special forensic software tools.[28] However, if offenders are using tools to ensure that files are securely deleted by overwriting the information, recovery is in general not possible.[29] Encryption technology is another common means of hindering investigations.[30] Such technology is not only increasingly common but increasingly effective.[31] The situation is a delicate one, for while encryption technology prevents law-enforcement agencies from accessing and examining often-critical information,[32] that very same technology is increasingly central to sustaining many of the things that societies around the world have come to consider as normal and necessary to daily life.[33]

Forensic experts can try to decrypt encrypted files.[34] If this is not possible, they can support law-enforcement agencies in developing strategies to gain access to encrypted files, for example by using a key logger.[35] Involvement in the collection of evidence includes the evaluation and implementation of new instruments. International cooperative efforts are particularly important in this regard.[36] One example of a new approach is the debate on remote forensic tools.[37] Remote forensic tools enable investigators to collect evidence remotely in real time[38] or to remotely monitor a suspect's activity[39] without the suspect being aware of investigations on his system. Where such tools are available, they can, on a case-by-case basis, play a decisive role in determining the best strategy for collecting e-evidence.

II. Assuring Authenticity, Integrity & Reliability

Having considered the nature of e-evidence and of computer forensics, the authenticity, integrity and reliability of the e-evidence needs to be assured by looking at **(A)** good practices for handling e-evidence, and **(B)** specific instances of the application of those practices.

A. Good Practices for Handling Digital Evidence

Good practices for handling e-evidence begin with **(1)** the development of a thorough and uniform forensic expert training program who alone handle e-evidence and **(2)** the creation of a nation-wide, e-evidence management system, the integrity of which is assured through copying techniques (taught in the training program).

1. Forensic Expert Training Program

The two most important examples of good practices for handling e-evidence are developing training programs for investigators and experts on techniques for identifying, handling and analyzing e-evidence. As with physical evidence, the authenticity, integrity and reliability of e-evidence can best be assured by giving due attention to (1) the examiner's expertise, (2) the reliability of tools and equipment and (3) the setting standardized procedures and guidelines:

1. **First, law enforcement should assure a specialized training and certification process for digital forensic examiners, and restrict the handling of any e-evidence to such examiners.** The approach might mirror that taken in the training of forensic scientists dealing with the physical evidence of a crime scene.[40] The procedural expertise of the examiner serves as a basis for inferring that the evidence has been handled with care, thereby assuring the integrity of the process—namely, that damage is avoided, alteration or manipulation prevented, and the outcome of the analysis verified. While courts do not generally require any specific training, certification or years of experience, a certain level is necessary to assure expertise. Moreover, just as with other certifications, recertification or continuing training courses are advisable.

2. **Second, the collection and analysis of e-evidence requires the use of a variety of tools and equipment.** Using widely-recognized tools (*e.g.*, software) and equipment[41] helps to warrant evidentiary reliability, and facilitates reexamination of evidence by outside experts. In addition to using such tools and equipment, however, standards exist for testing these forensic tools and equipment. A number of institutions can inspect ICT forensic tools and equipment. For instance, the US National Institute of Standards and Technology (NIST) provides standard testing methods for computer forensic tools and equipment through its Computer Forensics Tool Testing (CFTT) program.[42] Similar processes exist for the testing of other scientific equipment.

3. **Third, and lastly, standardized procedures and guidelines should be prepared and shared with anyone who might have cause to handle e-evidence.** Doing so creates a set, dependable methodology and approach, thereby helping protect against arbitrary handling of evidence. These rules should address handling of evidence at all stages of custody.

2. e-Evidence Management System & Copying Techniques

One of the greatest challenges related to e-evidence is the fact that it is highly fragile and can rather easily be deleted[43] or modified.[44] One consequence of its fragility is the need to maintain its integrity.[45] Case records are therefore required. In addition to training and qualifying experts in how to handle evidence, those experts should also be trained in the production of case records.[46] There are substantial advantages to storing those records should in a central, online e-evidence

management system that is accessible to certain, qualified law enforcement from around the country, if not world. Such a facility could be particularly important for storing data acquired in incidences where the seizure of hardware is impossible, inadequate or inappropriate, and where investigators have been permitted to copy files. That said, in addition to being difficult to roll-out to users beyond the capital, central systems can create high-profile targets and may represent a security vulnerability. Additionally, special attention needs to be paid to not only protecting the integrity of copied files against any kind of alteration during the copy process,[47] but also to the uploading process.

In incidences where devices and their original files are not taken into custody, and copies are made of those files, careful attention must be paid to assuring protocols for copying and uploading data for storage and analysis.

Methods called "imaging" and "hash-value generation" are used in demonstrating the authenticity of e-evidence.

- **Imaging** works in one of two ways, both of which rely upon the creation of a copied "image" of the e-evidence: either (1) by copying the digital data stored in an ICT device to create an image file using the bit-streaming method;[48] or (2) by producing a logic image file after selecting the files that are to be seized. Imaging allows investigators to preserve the authenticity of the image files be analyzed, as the data included in the files is not subject to change during the subsequent analysis.
- **Hash-value generation** works on the same logic of replicating the evidence in order to have a duplicate version to compare, understand, and analyze. However, rather than taking a duplicate image of the data, this technique relies on a file's so-called "hash value": much like a person's finger print or retinal image, the hash value is unique and inherent to each file. Therefore, reproducing the hash value reproduces the evidence. In a sort of cloning process, that hash value, which is derived from a hash algorithm, can be replicated along with the to-be analyzed file. As files that have the same hash value are regarded the same, the e-evidence is preserved by creating a copy.

Imaging and hash-value generation are both generally included in the e-evidence collection toolkit and used for on-site evidence collection. With replicas of the data in hand, investigators are then able to establish authenticity by imaging the seized ICT device itself. Veracity can be ascertained on-the-spot: the selected files are logic-imaged, their hash values generated and then the values produced compared with the hash values of the original evidence. That on-site verification is later submitted to the court.

B. Examples of Good Practices

Working along the lines of the good practices discussed above, the Supreme Prosecutors' Office of the Republic of Korea (KSPO) has established a **(1)** forensic expert training program and **(2)** centralized e-evidence management system.

1. The KSPO's Forensic Expert Training Program

A number of law enforcement agencies offer training programs not only for their ICT forensic experts but for any who might have cause to interact with e-evidence. One such example is the six-month digital Forensic Expert Training Program offered by the KSPO. An esteemed and competitive process, the KSPO selects a few trainees from a pool of regular investigators. Trainees receive three months of basic digital forensic training and another three months of on-the-job training in actual digital forensic divisions. Investigators who complete this six-month program are certified as "digital forensic investigators" and are subsequently placed in digital forensic divisions to collect and analyze e-evidence. As discussed above, the KSPO's program creates national uniformity and standardization of guidance, protocols and procedures, thereby helping to assure and convince the court of the authenticity, integrity and the reliability of e-evidence.

The Rule on the Collection and Analysis of Evidence by Digital Forensic Investigator is the KSPO's standard set of guidelines.[49] The Rule not only lays out the qualifications for becoming a digital forensic investigator, but also regulates procedure for on-the-crime-scene prodecures, setting down protocols for who is in charge of collecting and analyzing e-evidence, as well as articulating e-evidence search-and-seizure procedures, and data registration and management procedures for working with the Evidence Management System. The establishment of not only general guidelines but also concrete protocols and procedures make the KSPO's Rule an excellent example of good practices that go far towards protecting the authenticity, integrity and reliability of e-evidence.

2. Centralized e-Evidence Management System

Just as physical evidence collected by law enforcement is stored in a secured repository (often referred to as an "evidence room"), so, too, ought e-evidence to be securely stored in a central management system. Moreover, as e-evidence can be uploaded from multiple terminals, and even from various ICT devices, and as the limitations inherent to analogous physical evidence do not apply, e-evidence might—and should—be stored in one single, online repository, rather than in several disparate "evidence rooms".

The KSPO does as much, operating D-Net, its centralized, online evidence management system. Investigators register evidence collected from search-and-seizure and the results of conducted analysis directly into D-Net's central server. The system chronicles, registers and conserves the entire process. As such, D-Net preserves the entire chain of custody with respect to not only the e-evidence itself and its life cycle—collection, analysis, submission and disposal—but also work product. Crucially, it also allows for an established and secure means of timely data disposal.

III. Prosecution and Presentation

The investigation comes to a close with the presentation of evidence in court.[50] While presentation is customarily undertaken by prosecutors, forensic experts can play an important role in criminal proceedings as expert witnesses capable of assisting the triers of fact and of law to understand the evidence-collection procedures undertaken and the nature of the evidence subsequently generated.[51] Given the complexity of e-evidence, there is an increasing need to involve forensic experts.[52]

Although computer forensics deals to a large degree with computer hardware and computer data, it is not necessarily an automated process; indeed, while some processes, such as the search for suspicious keywords or the recovery of deleted files can be automated using special forensic analysis tools,[53] the vast majority of computer forensic examinations remains to a large extent manual work.[54] Such is especially true with regard to the development of strategies and the search for possible evidence within search and seizure procedures. The amount of time necessary for such manual operations and the ability of offenders to automate their attacks underline the challenges that law enforcement faces, especially in investigations involving a large number of suspects and large data volumes, and even more so when further complicated by cross-border activities.[55]

IV. The "Hearsay" Rule in Cybercrime

Some countries, such as the United Kingdom and Belgium, have special laws governing e-evidence that cover admissibility and authenticity of e-evidence.[56] In other countries, such as the United States and Korea, "traditional" rules of evidence (*i.e.*, the "hearsay rule") may be extended and applied.[57] The "hearsay" rule takes on a special form in cybercrime.

A. The "Hearsay" Rule

The hearsay rule is the basic evidentiary rule which provides assertions made by those outside of the court, and such derivative evidence, are generally inadmissible[58]; one of the most accepted legal definitions is "a statement not made in oral evidence in the proceedings that is evidence of any matter stated".[59] The rule has its origins in the notion that the trier of fact could only receive an objective, unbiased presentation of evidence if both sides have the same opportunity to confront the source of information (that is, through cross-examination).[60] As such, the evidentiary value rests on the credibility of the out-of-court asserter.[61] Essentially, the rule forbids notions of overheard evidence—that is, someone's testifying, "I heard him/her tell…"; or, "I heard say that…."[62]

Due to the confrontational style increasingly favored in the common law tradition, as opposed to the so-called "inquisitorial" style of the civil law tradition, the hearsay rule has a greater presence and bearing in the former tradition, with the civil law system being "far more receptive to derivative evidence generally".[63]

B. Korea's Treatment of the Hearsay Rule

The admissibility and authenticity of the electromagnetic record that forms e-evidence may be questioned if its printed form is submitted as evidence into courts. In some countries that do not have written regulations on these matters (*e.g.,* Korea), their highest courts may render decisions or judicial interpretations to address these issues. Such issues include the applicability of hearsay rule to determine authenticity and admissibility of such evidence.[64]

Case 2.12: Yeong Nam Committee Case (Korea)[65]

The Supreme Court of Korea has decided that the general hearsay rule, outlined in the Korean Criminal Procedural Law, does in fact apply to the authenticity and admissibility of e-evidence.[66] Applied to e-evidence, the rule was used to preclude the introduction as evidence of printed forms of digital files (*e.g.*, electronic documents; emails) saved in computers, servers or other storage devices. Although underscoring that a digitized document "is only different in terms of such document's recording media" and not "in substance […] significantly different" from a printed document containing the statements, the Court nonetheless excluded the presentation of the printed material out of concern for "the possibility of manipulation during the storage and printing process". As such, and with "no guarantee for cross-examination", the Court ruled that "the hearsay rule applies to authenticity of the content of a document recorded in digital files", and that, "under Article 313 (1) of the Criminal Procedure Act, it is admissible as evidence only when the writers (or 'the drafters') or the declarants (or 'the staters') statement authenticates it".[67]

As with evidence in general, the Court appears to be concerned with assuring the evidentiary chain of custody—that is, its authenticity, integrity and reliability—and, therefore, with demonstrating a proper showing of the printed page as an authentic representation of the original, e-evidence.

C. Exceptions to the Hearsay Rule

As with any rule, there are exceptions to the applicability of hearsay rules. Such examples might be implemented through various routes. Korea, which has been used as an example already, has introduced exemptions through both legislative and judicial mechanisms.[68]

In Korea, the legislative exception is rather limited and constrained; by contrast, the judicial exceptions have been more expansive. In the aforecited Korean Supreme Court's decision, a printed version of the digital file was deemed admissible only if its authenticity were established by the testimony of its asserter at a preparatory hearing to during a trial.[69]

In addition to such an exception, the Court has given several other exceptions to the general applicability of the hearsay rule:

1. **e-Evidence is not hearsay if digital file itself serves as a direct evidence of the offense.**[70] For instance, in texted phone messages creating fear or apprehension constitute direct evidence of crime in some countries criminalizing cyberstalking (*e.g.*, Korea);[71] or child pornography on a computer constitutes a direct evidence of crime in some countries (*e.g.*, USA).[72]

2. **e-Evidence is not hearsay if it is submitted to discredit the truthfulness of a statement, or where it is circumstantial evidence to an indirect fact.** For instance, evidence showing that a certain file was run can be used as circumstantial evidence to indirect facts.[73]

3. **e-Evidence that is automatically generated and which does not incorporate any thoughts or emotions is not hearsay.** For instance, network log records, web history, call history, GPS navigation information, file meta-information, etc. are all admissible on a showing of authenticity, integrity and reliability.[74]

Conclusion

Investigations must be prepared to turn into prosecutions if they are to have any effect. The evidentiary record, upon which adjudication must turn, being developed from e-evidence, specialized protocols and certifications ought to be developed. It is important that the established procedures, recognize the unique nature of e-evidence, and assure its authenticity, integrity, and reliability. In light of the fragility of e-evidence, law enforcement agencies must look for ways to preserve e-evidence throughout the entirety of the investigatory and prosecution process, from collection, through analysis and on to submission to court. Only trained and expert personnel, with digital forensic expertise, should handle e-evidence. All personnel should work according to established and standardized guidelines, procedures and protocols. Reliable, regularly-calibrated, and tested tools and equipment should be used, and all evidence, for the entire chain of custody—collection, analysis, submission and disposal—, should be uploaded to a central, online e-evidence management system.

Consideration should be given as to whether international recognition of evidence could be best facilitated by having an international body dedicated to developing certified training programs, as well as standardized procedures and guidelines. Such a body might be established in a manner similar to informal international information sharing and coordination centers (*see* section 4 B, below). That body, which, for example, might be housed within INTERPOL[75] or UNODC,[76] could

serve as a further vehicle for spreading good practices, as well as mitigating if not eschewing certain evidentiary concerns that might arise in cross-jurisdictional matters (*see* section 2 E, below).

In working with e-evidence, it is important to understand how the hearsay rule or similar exclusionary rules of evidence apply, as well as their exceptions. Hearsay rules exclude the admission of evidence that might result in bias or preclude the trier of fact's objectivity.

However, exceptions to hearsay rules may apply to e-evidence where there is no need to be concerned with bias, notably in the following circumstances:

1. When the digital file itself constitutes direct evidence of a crime;
2. When it is circumstantial evidence to an indirect fact; or
3. When the information automatically generated.

E. Jurisdictional Issues

Table of Contents

Introduction

The inherently transnational and cross-border nature of cybercrime renders investigating cybercrimes and prosecuting cybercriminals much more difficult than traditional crimes, largely due to the unique jurisdictional obstacles. Unlike their physical world analogs, cybercrimes can be committed from virtually anywhere on the globe, with attacks directed against targets in virtually any part of the world, and with effects potentially being felt by people the world over. For these reasons, states have found it necessary to reach beyond the territorial tethers that have been traditionally used to define sovereignty. While it is important to make space for the theoretical underpinnings to accordingly adapt to cyberspace, at the same time that increasingly-exerted ability of a targeted state to reach offenders beyond its territory must be balanced with respect for the sovereignty of other states.

Jurisdiction, understood in its basic sense as the official power to make legal decisions and judgments,[1] is a multi-faceted notion. Fundamentally, a state's jurisdiction is understood as being composed of three different authorities:

1. **Prescriptive authority –** that is, authority pertaining to the authority to impose laws;
2. **Adjudicative authority –** that is, authority pertaining to the authority to investigate and resolve disputes; and
3. **Enforceable authority –** that is, authority pertaining to the power to induce or punish pursuant to its prescriptive authority and subsequent to its adjudicative authority.

Typically, when speaking of a state having jurisdiction, it is with regard to all three of these facets (although, in exercising its authority, a court may apply the laws of another jurisdiction[3]). Three distinct areas of positive[4] jurisdictional conflicts exist: jurisdiction over the crime, over the evidence and over the perpetrator.

This section focuses principally on jurisdiction over the crime and then briefly on jurisdiction over the perpetrator. Further discussion of jurisdiction over the perpetrator and jurisdiction over evidence is discussed in sections covering procedural and evidentiary issues,[5] and in those covering the cross-border context.[6] This section discusses **(I)** traditional understandings of jurisdiction and **(II)** the adaptive jurisdictional principles that have emerged in international law. Thereafter, it turns to consider attempts to overcome jurisdictional issues **(III)** at the national level before **(IV)** briefly noting the utility of international instruments in extending that process.

I. The Traditional Notion of Jurisdiction

Jurisdiction of a state to criminalize an act has traditionally been based on its sovereign control over the specific territory in question—what is known as the principle of territoriality.[7] With such territorial control, the state is theoretically in a position to exert jurisdiction in its fullest extent for crimes occurring between people in that space, and to do so to the exclusion of all other powers: as the German sociologist Max Weber put it, the defining characteristic of the modern state is that it is a "human community that (successfully) claims the monopoly of the legitimate use of physical force within a given territory".[8] However, the nature of cyberspace often makes such a facile delineation of jurisdiction exceptionally difficult and even possibly nonsensical due to the inherent mobility, difficulty in proving location and geographic irrelevance in executing cybercrimes. Since a cybercrime can be perpetrated from entirely a country while having substantial effects within another country's borders, the traditional basis for jurisdiction has become inadequate, if not irrelevant.

Box 2.6: Inability to Prosecute Creator of the "Love Bug" Virus

On 4 May 2000, the so-called "Love Bug" virus (duly named because it was spread by opening an email bearing the title of "ILOVEYOU") rapidly "hopscotched" around the

world, affecting some fifty million people, from the US Pentagon to the UK Parliament, and costing an estimated US$10 billion worth of damages in a matter of hours.[9] The bug was programmed to replace all files with media extensions (images, documents, mp3s, etc.) with copies of itself, and then to send an identical email to all of the contacts of a victim's Outlook address book.[10]

Law enforcement traced the bug to the Philippines and identified a Filipino, Onel de Guzman, largely on the basis of an unusually heavy volume of data traffic to a computer located in the home of de Guzman's sister. The FBI and other authorities moved to take action against de Guzman. However, progress and prosecution was stymied by the fact that the Philippines did not, at that time, have laws governing computer crime (attempts were made to prosecute him under theft, but the charges were dropped due to insufficient evidence).[11] As such, the extradition treaties were rendered ineffectual due to the requirement of "dual criminality" (*see* section 2 A, above).

The "Love Bug" shows the limits of traditional notions of jurisdiction in cybercrime: an individual released a destructive antigen into cyberspace, causing damage and deleterious effects in some twenty countries, but, because he was physically located in a jurisdiction that had not criminalized such behavior, no action could be taken by the affected states.

II. Adaptive Jurisdiction Principles

Faced with the increasingly limited applicability of the traditional notion of jurisdiction to cybercrime, a series of adaptations have been developed, based principles of **(A)** territoriality, **(B)** active nationality, **(C)** passive nationality, **(D)** protection and **(E)** universality.

A. Principle of Territoriality

The principle of territoriality, the notion underpinning so much of our understandings of law, and especially for international law,[12] is the base principle for traditional claims of jurisdiction, as well as the basis upon which adaptive notions of jurisdiction are built.[13] The traditional understanding of jurisdiction operates on the conceit that the state inherently has complete jurisdiction over crimes occurring in its territory.[14]

This principle has been extended to nebulous yet quasi-territorial areas. Under the law of the flag (or the "flag principle"), vessels on the "high seas" (and those operating them) "possess" the nationality of the flag that borne by the vessel[15] (or where it is registered),[16] and thus that state has jurisdiction.[17] In 2014, the North Atlantic Treaty Organisation (NATO) deemed cyberspace to be sovereign domain akin to air, land and sea.[18]

The principle of territoriality has been used in other ways to alter traditional fixed methods and notions. For example, in one celebrated conflicts of law case, a New York court accepted jurisdiction over a tort matter that occurred outside of its territory, but in which both parties were New York residents; more interestingly, the court went on to apply New York law rather than the law of the place of the tort, as traditional rules would have dictated: the court made this deviation on the logic that the affected interests were in New York and had nothing to do with the other state.[19] Similarly, under an adaptive understanding of the principle of territoriality, a cybercrime "initiated" in the territory of one state but launched "at" another state, or made to occur "in", another state's territory gives the affected state jurisdiction.[20]

Another approach to this problem has been to broaden the notion of territoriality to extent to actions occurring in whole or in part in the prosecuting nation's territory.[21] Such an "occurrence" can be understood to include use of the affected state's infrastructure. Thus, this approach would give the state jurisdiction where both[22] or either victim or perpetrator are physically located in the state when the crime was committed,[23] or when any part of the crime was committed, planned or facilitated in that country.[24]

The principle of territoriality remains the principal basis for exerting jurisdiction over cybercrimes. The Budapest Convention, for example, makes it mandatory for signatories to adopt, legislatively or otherwise, all that is necessary for establishing jurisdiction over listed offences committed from within the state's physical territory.[25]

B. Principle of (Active) Nationality

Under the principle of nationality (or of active nationality), a sovereign may regulate the actions of its nationals abroad.[26] The principle is most typically invoked when a national commits a crime in a foreign state, and is more commonly found in the civil law tradition than in the common law tradition.[27] Under this principle, nationals of a state are obliged to comply with that state's domestic law even when they are outside of its territory.[28] When a national commits an offence abroad, the state is obliged to have the ability to prosecute if that conduct is also an offence under the law of the state in which it was committed.[29] In the instance of cybercrime, the principle is often relevant in child pornography cases, where the national attempts to perform the illegal action in a location where it is not a crime with the intent of distributing the subsequent material in his or her home country. The principle has less relevance in cybercrime than in other areas of criminal law as most cybercrimes can be effectuated from the perpetrator's home, while having cross border effects.[30]

C. Principle of Passive Nationality

The reciprocal of the principle of active nationality the principle of passive nationality (or passive personality). This principle applies where the national is the victim rather than the perpetrator,

thereby giving the state jurisdiction over the crime by which its national is victimized. The principle only takes on relevance when the entirety of the crime has occurred outside of the territory of the state. The principle is a controversial one, as it not only aggressively expands the notion of a state's authority, but, in so doing, it also implies that the law of the state with territorial jurisdiction is insufficient to remedy the wrong and incapable—or unwilling—to protect the interest of the victimized national.[31]

Case 2.13: LICRA v. Yahoo![32] (France) and Yahoo! v. LICRA (USA)[33]

Plaintiffs, *Union des Étudiants Juifs de France* ("UEJF") and *La Ligue contre la Racisme et l'Antisemitisme* ("LICRA"), brought a civil action against the French and American entities of Yahoo! over an internet auction of Nazi-period memorabilia under French criminal law, the "wear[ing] or exhibit[ing]" of Nazi paraphernalia is prohibited.[34] The French court of first instance ruled that there were sufficient links with France to give the court full jurisdiction, and proceeded to enjoin Yahoo! to take all necessary measures to dissuade and prevent French users from accessing the material in question—in other words, to block access to the online auction.[35] Although the competence of the French court was challenged and appealed in France, the original decision was upheld. Separate criminal proceedings in France were dismissed and defendants acquitted on all criminal charges; that a verdict that was upheld on appeal.

Following the French court decisions, Yahoo! brought suit in the United States, asking that the French judgment be deemed without effect in the United States.[36] The US District Court for the Norther District of California instead found that the French court's decision was inconsistent with US constitutional guarantees of freedom of expression. However, the US Court of Appeals for the Ninth Circuit reversed and remanded, with directions to dismiss the action on the divided basis of lack of ripeness and of lack of personal jurisdiction.[37]

D. Protective Principle

The protective principle (also called the "security principle" and "injured forum theory") is triggered when the crime—effectuated from beyond the state's territory—affects not just a national of the state, but a national security interest (domestic or international), such as the proper functioning of the government, or threatening the security of the state.[38] It is closely related to competition law's "effects doctrine" (or, as it is also termed, the "implementation test"),[39] which stipulates that where the economic effects of the anticompetitive conduct experienced on the domestic market are substantial, the affected state might exert jurisdiction over both foreign offenders and foreign conduct.[40] However, unlike both the effects doctrine and other forms of extraterritorial jurisdiction, the protective principle is not performed in an *ad hoc,* case-by-case fashion, but is instead used as

the basis for adopting statutes criminalizing extraterritorial behavior without regard to where or by whom the act is committed.[41] In the instance of the protective principle, neither perpetrator, nor victim, nor the implicated infrastructure are necessarily within the state. Such a tenuous, even weak, connection to the acting state, as well as to the significant,[42] often (at least partially) preemptive nature of the intrusion upon the sovereignty of the other state, makes extraterritorial exertions of jurisdiction based on this principle particularly controversial, and, as a result, probably the least used theory for sanctioning jurisdiction.[43]

E. Principle of Universal Jurisdiction

The principle of universal jurisdiction applies to specific crimes, but requires international—or universal—consensus: this principle recognizes a sovereign's right to adopt criminal laws restricting the behavior, regardless of who commits it, or where it is committed, insofar as restricting that conduct is recognized by nations as being of universal concern.[44] Piracy on the high seas, regarded as one of the first international crimes, is a classic example.[45] The use of this principle in cybercrime is limited because of the lack of consensus surrounding the criminality of cybercrimes.[46] However, and nonetheless, some states have extended universality to include certain cybercrimes—for instance, the German where the criminal code authorizes its authorities to prosecute all crimes of child pornography.[47]

III. National Frameworks

Regardless of whether international instruments are used to mitigate jurisdictional issues, national legal frameworks (*see* sections 5 A, and 5 B, below) might be crafted so as to facilitate cooperation. There are two means for a state to implement the above principles: either **(A)** by formally authorizing adaptive jurisdictional definitions through legislation, or **(B)** by relying on investigatory agencies to build relations—of varying degrees of formality—with their counterparts in other states. Both options, though different, are of great importance and value, each allowing for faster responses to concerns and better permitting the preservation of evidence.

A. Adaptive Legislative Jurisdictional Definitions

The first method that states might use to facilitate processes for obtaining jurisdiction over cybercrimes occurring beyond their territory is to legislatively authorize adaptive jurisdictional definitions discussed above.[48] Doing so formally extents the state's legal understanding of what constitutes criminal acts, even if conducted beyond that state's territory. In effect, it also puts would-be perpetrators on notice.

One such example of this approach is Australia's Criminal Code Act of 1995.[49] The Act's coverage of jurisdiction begins by building a broad basis of territorial jurisdiction ("standard geographical jurisdiction").[50] The Act provides four different classifications and situations authorizing Australian authorities with jurisdiction over a crime occurring beyond its territory ("extended geographical jurisdiction").[51] Furthermore, the Act stipulates that subsequent criminal legislation is to include a section stating what jurisdictional prescriptions apply.[52] By so legislating, Australia has acted "openly and notoriously", proclaiming to the world that it is at least entitled to exert jurisdiction beyond the immediate geographical borders.

B. Informal Cooperation

Additionally, or alternatively, states and authorities might address jurisdictional issues on a case-by-case basis through informal understandings and shared experiences of cooperation. Such is most typically done by law enforcement working directly with their counterparts in other states, therein in building informal bonds. Doing so often results in faster responses to requests for information sharing. The need for rapid information sharing is heightened at the investigatory stage, as authorities typically need to work quickly to prevent tampering or destruction of evidence; as already discussed, such is especially important for cybercrime. Informal cooperation is most common when dealing with child pornography and trafficking cases.

In order for this informal cooperation to be successful, trust must be built up over time through cooperation and personal ties. In the United States, the Computer Crime and Intellectual Property Section (CCIPS) has put forth a policy encouraging and fostering the building of such bonds.[53] Responsible for implementing the US DoJ's national strategies for combatting cyber and intellectual property crimes, CCIPS "prevents, investigates, and prosecutes computer crimes by working with other government agencies, the private sector, academic institutions, and foreign counterparts".[54] To this effect, CCIPS initiates and participates in international efforts.[55] The matter of informal international cooperation is addressed in greater depth further on (*see* section 5 B, below).

It bears noting that such bonds—the basic currency of diplomacy—need not be built exclusively by working on jurisdictional or even investigatory matters, but also through exchanges, shared trainings, and other periodic interactions. For instance, in early 2016, the world marveled at the successful agreement that the United States and Iran managed to reach in securing the release of ten US sailors captured by Iran after they strayed into Iranian territorial waters: the smooth resolution to a potentially fraught incident was attributed to the open communications channels between high-level representatives of each country that had been established during negotiations over Iran's nuclear program.[56] In that particular case, the personal connections that US Secretary of State John F. Kerry and Iranian Foreign Minister Javad Zarif had established allowed them to speak directly at least five times over a ten hour period.[57]

Even where formal instruments of international cooperation such as MLATs exist, informal cooperation is often essential to the successful investigation and prosecution of cybercrime. Major cybercrime cases frequently affect more than one country—for example, when administrators of website selling stolen credit cards are arrested. In such cases, several states may be in a position to exert jurisdiction. However, weighing the particularities and appropriateness is often beyond the scope or means of MLATs. For instance, rather than take on the matter directly, the Budapest Convention simply provides that, if appropriate, countries consult with each other to decide which state should assert jurisdiction.[58] At such a crossroads, informal understandings and relationships often play a larger role in determining the expediency with which matters proceed. Indeed, when more than one country is interested in a case, law authorities of the affected states will already be collaborating before any turning point, such as an arrest, is reached. Thus, even if several countries could claim jurisdiction, there may in fact be no dispute. These informal cooperative arrangements are often the best milieu for considering which and whether targets will be tried in one country or another (perhaps on the basis of which sentences are traditionally heavier), or on the order in which prosecution and sentencing will occur.

IV. Multilateral Instruments

Where cybercriminal matters are concerned, negotiated multilateral instruments—rather than the afore-discussed jurisdictional theories—are the most effective and important means of establishing extra-territorial jurisdiction. International instruments are essential to combatting cybercrime as jurisdictional issues arise frequently and in all forms. As such, international cooperation is crucial to building effective, comprehensive legal frameworks to combat cybercrime.

While international cooperation comes in various forms, the two most common forms MLATs and extradition treaties, both of which are discussed in greater depth further on (*see* section 5 A, below). It bears noting that the issue of convergence of legislation is highly relevant, as a large number of countries base their MLA regime on the principle of dual criminality.[59]

Conclusion

Although there are a number of offences that can be prosecuted anywhere in the world, regional differences play an important role. Cybercrime offenses cannot be properly prosecuted within the confines of traditional understandings of jurisdiction. Due to the transnational nature of cybercrimes, states need to create means for investigating and prosecuting offenses which target or affect them and which occur, or which are launched, from beyond their borders. Such begins by developing comprehensive national legal frameworks. However, jurisdictional extensions meet, and therefore must balance with, the sovereignty of other states. A diversity of legal bases exists

for exerting jurisdiction, the most important of which is the territorial principle and its adaptive notions.[60]

To best deal with the jurisdictional issues arising from cybercrimes, states need to both develop inclusive definitions of jurisdiction and work on furthering international cooperation in investigations and prosecutions. Increasing reliance on MLATs and on extradition treaties will assist such a process, but those international instruments can only have full effect insofar as states develop adaptive legal national frameworks. Indeed, the biggest obstacle to prosecuting cybercrimes is the dual criminality requirement. As the dual criminality requirement is important on many levels, international cooperation is needed so that similar cybercriminal legislation—at least on what constitutes cybercrime offenses—is implemented.

It bears noting that establishing jurisdiction over the crime opens the door to other issues. A state having acted formally through legislation to extend its jurisdictional ambit is confronted by two subsequent challenges: first, as already discussed, that of acquiring personal jurisdiction over the perpetrator; and, second, that of having sufficient capacity to investigate the crime, a matter that is significantly complicated by the fact that the crime occurred beyond its own territory. Both of these complications are best addressed by further developing not only formal levels of cooperation, but also informal ones.

F. Institutional Framework

Table of Contents

Introduction

As discussed,[1] effectively fighting cybercrime begins by creating a legal framework, which begins with effective legislation and subsequent executive action. That framework must create space for PPPs and increase public awareness. Building upon the basis of that legal framework, the fight against cybercrime requires an institutional framework that allows for inputs and communications between and among both national and international groups and agencies, and which provides at least a base of commonality for policies, procedures, and processes.

This section addresses some good practices in building institutional frameworks to combat cybercrime by **(I)** creating a national cybersecurity strategy (NCS) for safely structuring, shaping, and developing cyberspace, and by **(II)** dealing with how to most effectively organize authorities charged with various and often overlapping aspects cyberspace.

I. National Cybersecurity Strategy

There is a strong global trend towards developing national cybersecurity strategies, with dozens of countries across the globe already having done so.[2] As such, there is now substantial guidance—from both national and international sources—for those countries looking to create and tailor

a national cybersecurity strategy to fit their own unique circumstances and exigencies. This subsection looks at **(A)** various aspects that go into forming a comprehensive and effective national cybersecurity strategy, and **(B)** considers an example of good practice.

A. Creating a National Cybersecurity Strategy

NCSs are strategic approaches that help states to mobilize and orchestrate resources to comprehensively and efficiently understand what cyberspace means for them, and to prepare to face threats coming from that space. An effective NCS is cross-dimensional and cross-cutting, speaking to questions of policy, cybersecurity's larger societal place and the nature of that society. An NCS creates a broad, strategic framework by which relevant government agencies can carry out national policies, thereby implementing a nationally consistent and systematic cybersecurity policy. It is typically aspirational and propositional, requiring subsequent implementation. It comprehensively touches upon all of the diverse factors pertaining to national cybersecurity, such as specialized investigative units, increasing general institutional capacity, coordinating various agencies, supporting knowledge-sharing and operational exchanges., As cybersecurity is a shared responsibility that requires coordinated action from government authorities, the private sector and civil society, an NCS also seeks to raise public awareness of cyber threats and how such incidents might be prevented, as well as looking to limit proliferation of cyber weapons, thereby facilitating prompt response and recovery to attacks. Countermeasures to cybercrimes might also be discussed.

The NCS should be both inward and outward looking. The strategy must consider how best to mobilize and coordinate diverse and disparate internal actors, ranging from law enforcement agencies to those involved in the nation's infrastructure (*e.g.*, power grid, roads, dams). Doing as much demands cooperation among all parties, private and public. For instance, one of the reasons that the alleged US cyberattack on North Korea failed (in contrast to the Stuxnet cyberattack launched against Iran)[3] was North Korea's severe internet and communications isolation, as well as the utter secrecy imposed by the regime.[4] This situation is highlighted as indicative of the fact that securing cyberspace requires much more than the mere increase of activity by law enforcement; Moreover, freedom of information and freedom a free, fluid cyberspace being beneficial to society at large, it bears making it explicit that the authors are not advocating for the severe, dictatorial measures imposed by the North Korean government. The NCS should not only be inward but also must also be outward looking. It should be prepared with sufficient flexibility to facilitate collaboration with other national and international institutions. Moreover, the NCS should account and facilitate both formal and informal international inputs (*see* sections 5 A and 5 B).

Part of the strategy should have an office serving as a "control tower" role, both for implementing and monitoring the strategy's implementation, as well as for carrying on operations thereafter. Such a centralized office is particularly important for coordinating among the diverse actors. This office is crucial to effectively should bringing together all of the diverse elements that might be implicated

in fighting cybercrime; while space for improvisation should be allowed, those elements should be laid out in the NCS itself, rather than being left in an *ad hoc* fashion to the office. To facilitate and build momentum, a timeline is typically included.

Given the disparate and developing elements covered, certain states have taken a fragmented approach, forming the NCS not of one document but of several. Such is not necessarily problematic, insofar as the fragmented elements forming the NCS can be clearly and coherently pieced together without effort or confusion.[5]

B. An Example of Good Practice

The United Kingdom's *Cyber Security Strategy,* published on 25 November 2011, provides an example of good practice in developing a NCS.[6] The Strategy begins broadly, being introduced as "set[ting] out how the UK will support economic prosperity, protect national security and safeguard the public's way of life by building a more trusted and resilient digital environment".[7]

The Strategy proceeds by setting out its *raison d'être* in four large and basic goals that implementation is hoped to accomplish:

1. **Tackling cybercrime,** thereby making Britain one of the most secure places in the world to do business in cyberspace;
2. **Increasing cyberattack resilience,** thereby increasing the Britain's ability to protect interests in cyberspace;
3. **Helping shape and open-up cyberspace,** thereby making it a stable and vibrant space in which the public can safely operate, therein contributing to an open society;
4. **Eliminating silos,** thereby creating cross-cutting knowledge, skills, and capability needed to underpin cybersecurity at large.

These four, overarching goals—intended to deliver the Strategy's vision of "a vibrant, resilient and secure cyberspace"[8]—are divided into fifty-seven discreet, manageable tasks covering a full range of issues, including strengthening law enforcement agencies, examining current laws, sharing information on cyber threats, adopting new procedures for responding to cyber incidents and strengthening international cooperation.[9] Each task is assigned to one of the following six British agencies in charge of the Strategy's implementation: the Home Office,[10] the Department for Business, Energy and Industrial Strategy (BEIS),[11] the Department for Culture, Media and Sport,[12] the Cabinet Office,[13] the Ministry of Defence[14] and the Foreign and Commonwealth Office (FCO).[15] The Strategy's publication in 2011 led to a four-year implementation period. Momentum was maintained through annual progress reports, with the Cabinet Office's Office of Cyber Security and Information (OCSI) operating as the appraisal and management center.[16] At a cost of GB£860 million to date,[17] and with the government having committed a further GB£1.9 billion over the next five years to cybersecurity,[18] the Strategy is a robust commitment.

II. Organizing Agencies

Just like the physical world, safely structuring, shaping, and developing cyberspace so that all might benefit requires the input of a diversity of actors. As such activity often results in overlapping competencies and authorities, it is important for states to develop an institutional framework by **(A)** laying out a comprehensive NCS that addresses the vast array of cyberspace issues and by **(B)** facilitating knowledge sharing among the actors, such as through the creation of joint taskforces.

A. Dealing Overlapping Authorities

A comprehensive NCS goes well beyond cybercrime and cybersecurity, encompassing a variety of cyberspace issues. It should discuss and develop not only the country's larger vision and policy issues, but also should explore approaches for promoting ICT development, implementing regulations on the misuse of technology, finding solutions to privacy concerns and exploring the development of investigative and prosecutorial procedures. Due to the cross-cutting nature of cyberspace and of such concerns, various government agencies and offices necessarily handle these issues. While each agency should, in accordance with its own mandate, carry out its own tasks, a timeline and plan for coordinating efforts and for facilitating inter-agency cooperation is crucial to effective strategy implementation.

Broadly speaking, the development of cyberspace can be divided into four areas:

1. **ICT policies** (*e.g.*, regulation, development);
2. **Cybersecurity** (*e.g.*, infringements, certifications);
3. **User protection** (*e.g.*, protecting privacy, personal information); and
4. **Cybercrime** (*e.g.*, combatting, investigating, prosecuting).

In mapping responsibilities, it is important that agency roles and responsibilities be clearly assigned. Doing so will allow for the discreet handling of issues, therein avoiding confusion and overlap, as well as facilitating resource allocation and nurturing the development of expertise. Furthermore, the institutional framework should support the legislative and executive mandates created under the legal framework, appropriately assigning specific roles to various agencies. In order for the overall institutional framework to function properly, it is essential that involved agencies constantly engage in self-critical evaluation procedures, as supported and supervised by a central, "control tower" office. An essential part of this process depends upon appropriate feedback loops that the central office must consider.

An example of the clear assigning of tasks can be found in the United Kingdom, as discussed above; a more detailed breakdown of the Korean experience follows:

Table 2.1: Relevant Cyberspace Laws and Administering Agencies

Categories	Agencies in Charge	Relevant Statutes
Information Communications Policies	■ Ministry of Science, ICT and Future Planning ■ Korea Communications Commission	■ Act on Promotion of Information and Communications Network Utilization and Information Protection ■ Digital Signature Act ■ Act on the Protection, Use, etc., of Location Information ■ Telecommunications Business Act
Cybersecurity	■ Ministry of Science, ICT and Future Planning (for the private sector) ■ KrCERT ■ National Intelligence Service (for the public sector)	■ Act on the Protection of Information and Communications Infrastructure ■ Act on Promotion of Information and Communications Network Utilization and Information Protection
User Protection	■ Ministry of Interior ■ Korea Communications Commission ■ Financial Services Commission	■ Personal Information Protection Act ■ Act on Promotion of Information and Communications Network Utilization and Information Protection ■ Special Act on Refund of Amount of Damage Caused by Telecommunications Bank Fraud
Cybercrime	■ National Police Agency ■ Prosecutor's Office ■ Ministry of Justice	■ Criminal Act ■ Criminal Procedure Act ■ Protection of Communications Secrets Act

As the above table indicates, various acts and agencies play a role in regulating cyberspace. For example, the Act on Promotion of Information and Communications Network Utilization and Information Protection (APICNU), a major statute in Korea's information communications sector, has as its purpose "to promote the utilization of information and communications networks, to protect the personal information of users utilizing information and communications services, and to build a safe and sound environment for the information and communications networks in order to improve the citizen's lives and enhance the public welfare."[19] The two competent authorities for this Act are the Ministry of Science, ICT and Future Planning (MSIP) and the Korea Communications Commission (KCC). MSIP mainly deals with facilitating utilization of ICT and maintaining cybersecurity in the private sector, while KCC is in charge of regulating the telecommunications business and of protecting personal information in the information communications network. However, while both MSIP and KCC are the major institutional players, for certain violations, the APICNU provides criminal sanctions, the triggering of which shifts authority away from MSIP and KCC to those agencies generally charged with investigative and prosecutorial roles.

Power sharing schemes similar to that of the APICNU exist both in most of the other Korean laws, as well as in the laws of many other states. As such, it is all the more important that both a clear institutional framework and a targeted NCS be developed, with competencies and responsibilities being clearly assigned and delineated on the basis of the legal framework.

B. Knowledge Sharing & Joint Taskforces

Knowledge sharing is a key corollary to any power-sharing scheme, regardless of how formal or informal. Just as a certain degree of flexibility and imprecision should be left in the law in order to accommodate the fast-paced and ever-evolving nature of cybercrime, it is also important that assignations of power not be excessively limiting, and that appropriate inter-agency and inter-departmental communication plans and paths be opened and employed. While the cybersecurity "control tower" office can facilitate information sharing, it is important that each agency realizes and acts on the understanding that information on threats can come through different routes, thereby facilitating investigation, prosecution and overall threat detection.

One way of connecting various agencies is through joint investigative taskforces. In forming joint taskforces, each participating agency assigns contact officers to the joint taskforce. In certain cases, those officers may even be seated in the same physical location or otherwise obliged to maintain frequent contact, and may even jointly participate in criminal investigations. A joint taskforce might be organized on a temporary basis in order to resolve a particular case, or established on a more permanent basis. In any case, longer-term arrangements that open up regular channels of communications, and which encourage direct and frequent interactions between agency point persons are helpful in developing a continuous cooperative system between the agencies.

Joint taskforces are used by a number of countries. For instance, in the United States, the DoJ has organized the National Cyber Investigative Joint Task Force (NCIJTF) under the purview of the FBI Cyber Division. Separately, the Department of Homeland Security (DHS) has organized more-disparate and localized the Electronic Crimes Task Forces (ECTFs) under the auspices of the Secret Service.[20] Formed in 2008, the NCIJTF is the primary US agency responsible for coordinating cyber threats investigations and liaisons among the FBI, Central Intelligence Agency (CIA), Department of Defense (DoD), DHS, and NSA.[21] The ECTFs, originally created in New York in 1996 to combine the resources of academia, the private sector and local, state, and federal law enforcement agencies in combating computer-based threats to the nation's financial payment systems and critical infrastructures,[22] was expanded by federal legislative action[23] to create a nationwide network (with two offices abroad) that focuses on identifying and locating international cyber criminals connected to cyber intrusions, bank fraud, data breaches, and other computer-related crimes.[24]

Similarly, in Korean, the KSPO established the Joint Personal Information Investigation Team (JPIIT) in April 2014 following the theft of extremely sensitive personal data—including identification numbers, addresses and credit card numbers, which affected over twenty million South Koreans

equal to roughly forty percent of the population.[25] While the massive breach on Target Corporation was due to malware on point-of-sale systems,[26] the Korean banks were compromised by a third-party worker; these two disparate cyberthreats underscore the wide variety of threats facing consumers.[27]

JPIIT is composed of personnel from eighteen different groups, eleven of which are government agencies and six of which come from the private sector. Different types of tasks are assigned to different agencies. For instance, private actors, including the Online Privacy Association (OPA), communications companies and portal companies, deal with collecting and analyzing illegal personal information. Additionally, the Korean Internet and Security Agency (KISA) deals with infringements. The Ministry of the Interior deals with inspecting personal information security. KSPO and the National Police Agency handle investigations and prosecution. The National Tax Service addresses recovery of criminal proceeds. The Ministry of Strategy and Finance (MOSF), MSIP and the Personal Information Protection Commission (PIPC) address the improvement of policy and regulation. Supervising business communications is done by the Financial Services Commission (FSC) and the Financial Supervisory Service (FSS) supervises the finance sector, while MSIP and the Korea Communications Commission (KCC) supervises communications in the ICT sector.

Crucially, JPIIT sits with the High-Tech Crimes Investigation Division 1 of the Seoul Central District Prosecutor's Office. As this Division is charged with investigating cybercrimes, the joint taskforce participates both directly and indirectly in cybercriminal investigations, should matters escalate to such a level. The participation of a diversity of actors, and the intense degree of information sharing between them, facilitates management of tasks pertaining to personal information, be it the prevention and monitoring of personal information crimes, investigation and prosecution or the recovery of criminal proceeds. Because JPIIT operates at the case-intake point, members can immediately report to their respective agencies upon encountering an issue that falls under their group's particular purview.

Private sector actors play a crucial role in JPIIT by collecting various types of illegally distributed personal information from their regular business operations and handing them over to law enforcement agencies. In so doing, the methods in which cybercriminals use the information system is better understood and directly reported to law enforcement, thereby facilitating repair of vulnerabilities at the earliest stage possible.

Conclusion

Countries are increasingly establishing NCS as part of their institutional frameworks. Doing so facilitates a robust, organized and structured response to insecurity in cyberspace. These strategies contribute to mobilizing government action—by eliciting wider agency participation, facilitating capacity building and knowledge sharing and helping to assure consistent implementation of

cybersecurity policies—, while also facilitating public awareness and engagement. Strategy implementation can be facilitated and accelerates by designating an office to manage and periodically assess progress.

The institutional framework should take a holistic approach to dealing with cyberspace. As so many divergent actors are required to safely structure, shape, and develop cyberspace for everyone's benefit, it is vital to share accumulated information and expertise. Joint investigative task forces that bring together relevant actors: agencies involved in systems' administration, as well as investigatory and prosecutorial proceedings, need to be brought together on a regular basis. Space should also be made to periodically bring key private sector actors, such as data privacy groups and ISPs, to the table.

End Notes

Referenced in: § A. Working Definition of Cybercrime

1. Brenner, "Thoughts, Witches and Crimes," *supra* § 1 B, note 2.

2. "Cybercrime refers to any crime that can be committed by means of a computer system or network, in a computer system or network or against a computer system. In principle, it encompasses any crime capable of being committed in an electronic environment." *Background Paper for the Workshop on Crimes Related to the Computer Network,* 10th UN Congress on the Prevention of Crime and the Treatment of Offenders, (10–17 Apr. 2000) A/CONF.187/10, [hereafter, "UNODC Conference Paper"] p. 4, at https://www.unodc.org/documents/congress//Previous_Congresses/10th_Congress_2000/017_ACONF.187.10_Crimes_Related_to_Computer_Networks.pdf.

3. UN Secretariat, "Background Paper: Workshop 3 on Strengthening Crime Prevention and Criminal Justice Responses to Evolving Forms of Crime, Such as Cybercrime and Trafficking in Cultural Property, Including Lessons Learned and International Cooperation," 13th UN Congress on Crime Prevention and Criminal Justice, (2 Feb. 2015) A/CONF.222/12, p. 6, at http://www.unodc.org/documents/congress/Documentation/A-CONF.222-12_Workshop3/ACONF222_12_e_V1500663.pdf.

4. In addition, a cybercrime may be prosecutable under the general criminal code. A standard forgery statute may stretch to cover electronic forgery, theft via electronic systems may be covered by a standard theft statute, and so on.

5. COMSEC, "Report of the Commonwealth Working Group on Experts on Cybercrime," Meeting of Commonwealth Law Ministers and Senior Officials, Gaborone, Botswana (5–8 May 2014), Annex A, pp. 13–14, at http://thecommonwealth.org/sites/default/files/news-items/documents/Report_of_the_Commonwealth_Working_Group_of_Experts_on_Cybercrime_May_2014.pdf.

6. *See, e.g.,* Wall, "Policing Cybercrimes," *supra* § 1 B, note 33.

7. On the basis of the legal principle of *nulla poena sine lege* (Latin for "no penalty without a law"), it is generally understood that crimes must be defined with appropriate certainty (legal certainty) and definiteness (both in the committed act and the requisite mental state), and with appropriate notice given, in order for the rule of law to exist.

8. Generally speaking, laws are interpreted by courts according to their "plain" or "literal" meaning, by which judges are to read the letter of the law in a textual, word-for-word sense without diverting from its true meaning, with words given their plain, ordinary and literal meaning. *See, e.g.,* United Kingdom: *Fisher v Bell* [1961] 1 QB 394; United States: *Connecticut Nat'l Bank v. Germain,* 112 S. Ct. 1146, 1149 (1992). The rule of "narrow" or "strict" construction of criminal statutes, the opposite of "liberal" or "broad" construction, means that a criminal statute may not be expanded by implication or intent beyond the fair meaning of the statute's language; its corollary, the rule of lenity, holds that ambiguity should be resolved in the defendant's favor. *See, e.g., United States v. Granderson,* 114 S. Ct. 1259, 1263 (1994). The result of this approach is that "when choice has to be made between two readings of what conduct [a legislature] has made a crime, it is appropriate, before [choosing] the harsher alternative, to require that [the legislature] should have spoken in language that is clear and definite." *Dowling v. United States,* 473 U.S. 207, 214 (1985) (internal quotations and citations omitted).

9. Basic information on international and regional instruments on cybercrime is provided in appendix 9 A (Multilateral Instruments on Cybercrime).

10. Oxford English Dictionary.

11. UNODC Cybercrime Study, *supra* § 1 B, note 7.

12. *See, e.g.,* Budapest Convention, *supra* § 1 B, note 32, at Art. 1.b.

13. *Ibid. See also,* ITU Understanding Cybercrime, *supra* § 1 B, note 1, at 11 & 41 ("For example, a person who produces USB devices containing malicious software that destroys data on computers when the device is connected commits a crime."); UNODC Cybercrime Study, *supra* § 1 B, note 7 ("In practice, computer data or information likely includes data or information stored on physical storage media (such as hard disk drives, USB memory sticks or flash cards), [….]").

14. *See, e.g.,* League of Arab States, *Arab Convention on Combatting Information Technology Offences* (21 Dec. 2010), [hereafter, "Arab Convention"], Art. 2(6); Budapest Explanatory Report, *supra* § 1 D, note 14.

15. CoE's Cybercrime Convention Committee (T-CY) notes that "the definition of 'computer system' in Article 1.a [of the Budapest Convention] covers developing forms of technology that go beyond traditional mainframe or desktop computer systems, such as modern mobile phones, smart phones, PDAs, tablets or similar". "Guidance Note # 1: On the Notion of 'Computer System': Art. 1.a, Budapest Convention," adopted by the T-CY at its 8th Plenary, (5 Dec. 2012) CoE, T-CY at https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e79e6. UNODC Cybercrime Study, *supra* § 1 C, note 7 ("Based on the core concept of processing computer data or information, it is likely that provisions typically apply to devices such as mainframe and computer servers, desktop personal computers, laptop computers, smartphones, tablet devices, and on-board computers in transport and machinery, as well as multimedia devices such as printers, MP3 players, digital cameras, and gaming machines.").

16. Kristin Finklea & Catherine A. Theohary, "Cybercrime: Conceptual Issues for Congress and Law Enforcement," US Congressional Research Service (CRS), (15 Jan. 2015), p. 3, at https://fas.org/sgp/crs/misc/R42547.pdf.

17. *See supra* § 1 C.

18. "An Electronic Trail for Every Crime," Homeland Security Newswire, (19 Apr. 2011), at http://homelandsecuritynewswire.com/electronic-trail-every-crime.

19. Sarah Gordon & Richard Ford, "On the Definition and Classification of Cybercrime," Journal of Computer Virology, Vol. 2 (2006), pp. 15–19.

20. John Lasseter, dir. *Toy Story*. Walt Disney Pictures & Pixar Animation Studios. 1995. Film.

21. ITU, "Overview of the Internet of Things," Recommendation ITU-T Y.2060 (Jun. 2012), Internet of Things Global Standards Initiative, at http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=y.2060. *Cf.* US Federal Trade Commission (FTC), "Internet of Things: Privacy and Security in a Connected World," FTC Staff Report, (Jan. 2015) [hereafter, "FTC Report"], at https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

22. *Ibid. See, also,* "Internet of Things (IoT)," Cisco, at http://www.cisco.com/c/en/us/solutions/internet-of-things/overview.html.

23. "How Hackers Could Use Doll to Open Your Front Door," BBC News, (14 Feb. 2017), at http://www.bbc.com/news/technology-38966285.

24. *See, e.g.,* FTC Report, *supra* note 21.

25. *See, e.g.,* Luke Simmons, "What Is the Difference between the Internet of Everything and the Internet of Things," CloudRail, (14 Oct. 2015), at https://cloudrail.com/internet-of-everything-vs-internet-of-things/.

26. *See, e.g.,* Tim Bajarin, "The Next Big Thing for Tech: The Internet of Everything," Time, (13 Jan. 2014), at http://time.com/539/the-next-big-thing-for-tech-the-internet-of-everything/.

27. *See, e.g.,* "Intelligent Machines Quantum Computing Now Has a Powerful Search Tool," MIT Technology Review, (5 Apr. 2017), at https://www.technologyreview.com/s/604068/quantum-computing-now-has-a-powerful-search-tool/.

28. *See, e.g.,* Avaneesh Pandey, "Energy-Efficient 'Biocomputer' Provides Viable Alternative to Quantum Computers," IBT, (28 Feb. 16), at http://www.ibtimes.com/energy-efficient-biocomputer-provides-viable-alternative-quantum-computers-2326448.

29. Alex Hern, "Google Says Machine Learning Is the Future. So I Tried It Myself," Guardian, (28 Jun. 2018), at https://www.theguardian.com/technology/2016/jun/28/google-says-machine-learning-is-the-future-so-i-tried-it-myself/.

30. *See supra* § 1 C for a discussion of the debate on the strength of encryption.

31. David R. Johnson & David Post, "Law and Borders: The Rise of Law in Cyberspace," Stanford Law Review, Vol. 48 (May 1996), 1367, at https://cyber.harvard.edu/is02/readings/johnson-post.html.

32. The basis for international public law is by and large built upon the notion of the sovereignty of the Westphalian state. *See, e.g.,* Andreas Osiander, "Sovereignty, International Relations, and the Westphalian Myth," International Organization, Vol. 55 (2001), p. 251–87. For a fuller discussion, *see infra* § 2 E.

33. *See* Johnson & Post, *supra* note 31, at p. 1379.

34. BI Intelligence, "Samsung Is Building a Smart Cities Network in South Korea," Business Insider, (25 May 2016), at http://www.businessinsider.com/samsung-is-building-a-smart-cities-network-in-south-korea-2016-5.

35. *See, e.g.,* "Brief: Smart Cities," World Bank (8 Jan. 2015), at http://www.worldbank.org/en/topic/ict/brief/smart-cities; Smart Cities Council, at http://smartcitiescouncil.com/.

36. *See, e.g.,* European Network of Living Labs, at http://www.openlivinglabs.eu/.

37. *See* Johnson & Post, *supra* note 31, at p. 1369.

38. *See supra* § 1 A. *See also* Shearer, *Extradition in International Law,* (Manchester: Manchester University Press, 1971), p. 137; Schultz, "The Great Framework of Extradition and Asylum," in Treatise on International Criminal Law, Vol. 2 (1973), p. 313.

39. *See* FTC Report, *supra* note 21.

40. *See* infra § 2 E. *See also* Sunil Kumar Gupta, "Extradition Law and the International Criminal Court," Berkeley Journal of Criminal Law, VOl. 3 (2000), at http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1072&context=bjcl.

41. *See, e.g.,* "Long-Arm Statute," LII, Cornell University Law School, at https://www.law.cornell.edu/wex/long-arm_statute.

42. "Cybercrime," INTERPOL, at http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime.

43. UNODC Conference Paper, *supra* note 2.

44. *Ibid.*

45. *See, e.g.,* Portugal: Cybercrime Law, Law No. 109 (15 Sep. 2009), Art. 11, at http://www.wipo.int/edocs/lexdocs/laws/en/pt/pt089en.pdf.

46. *Supra* Budapest Convention, *supra* § 1 B, note 32 and Arab Convention, *supra* note 14.

47. CIS, *Agreement on Cooperation among the States Members of the Commonwealth of Independent States (CIS) in Combating Offences Related to Computer Information* (2001) (entered into force on 14 Mar. 2002) [hereafter, "CIS Agreement"], Art. 5, at https://cms.unov.org/documentrepositoryindexer/GetDocInOriginalFormat.drsx?DocID=5b7de69a-730e-43ce-9623-9a103f5cabc0.

48. African Union, *African Union Convention on Cyber Security and Personal Data Protection,* EX.CL/846(XXV) (27 Jun. 2014) [hereafter, "AU Convention"], Art. 28, para. 1 & 2, at http://pages.au.int/infosoc/cybersecurity. The AU Convention is also sometimes referred to as the "Malabo Convention". Although a positive step in the progress of the fight against cybercrime, the AU Convention is deficient in certain areas. *See, e.g.,* Mailyn Fidler, "The African Union Cybersecurity Convention: A Missed Human Rights Opportunity," Council of Foreign Relations Blog, (22 Jun. 2015), at http://blogs.cfr.org/cyber/2015/06/22/the-african-union-cybersecurity-convention-a-missed-human-rights-opportunity/. This matter is discussed in greater depth further on; *see infra* § 5 A.

49. UNODC Cybercrime Study, *supra* § 1 B, note 7.

50. *See e.g.,* United Kingdom: Computer Misuse Act, 1990.

51. *See, generally* appendix 9 C.

52. As indicated in appendix 9 C, 196 countries are targeted. As of 2 October 2015, approximately 76.0% (149 countries) have domestic law that comprehensively or partially governs cybercrime irrespective of having draft law on cybercrime. Specifically, 137 countries adopted domestic law that holistically or partly covers cybercrime, and another 12 countries had or have a draft law that deals with cybercrime, along with having other laws that address cybercrime. Further, 12 countries had or have a draft cybercrime law in progress. However, 33 countries have no domestic legislation pertaining to cybercrime, while 2 countries have no data to assess their legislative statuses.

53. Examples of domestic law concerning cybercrime whose name explicitly uses the term "cybercrime" can be found in, among others, Botswana, Cybercrime and Computer Related Crimes, 2007 and Philippines, Cybercrime Prevention Act, (2012).

54. *See* Russia: Criminal Code, ch. 28, Crimes in the Sphere of Computer Information, at http://www.wipo.int/edocs/lexdocs/laws/en/ru/ru006en.pdf.

55. A list of domestic legislation regarding concerning cybercrime whose name provides the term similar to "cybercrime" includes, but is not limited to, Antigua and Barbuda: Electronic Crimes Act, (2013); Sri Lanka: Computer Crime Act, (2007); Bahrain: Law concerning Information Technology Crimes, (2014); and Dominican Republic: Law on High Technology Crimes, (2007).

56. *See, e.g.,* China: Criminal Law, (2016), Art. 286 ("Whoever, in violation of State regulations, cancels, alters, increases or jams the functions of the computer information system, thereby making it impossible for the system to operate normally, if the consequences are serious, shall be sentenced to fixed-term imprisonment of not more than five years or criminal detention."). *See, e.g.,* Abhishek Pratap Singh, "China's First Cyber Security Law," Institute for Defense Studies and Analyses, (23 Dec. 2016), at http://www.idsa.in/backgrounder/china-first-cyber-security-law_apsingh_231216#footnote5_w4sr2kl.

57. *See, e.g.,* Oman: Royal Decree Issuing the Cyber Crime Law, (2011), which states that "cybercrime refers to crimes referred to in this law," at http://www.qcert.org/sites/default/files/public/documents/om-ecrime-issuing_the_cyber_crime_law-eng-2011.pdf.

58. *See, e.g.,* Kosovo: Law on Prevention and Fight of the Cyber Crime (2010), Art. 3, which defines "cybercrime" as a criminal activity carried out in a network that has as objective or as a way of carrying out the crime, misuse of computer systems and computer data, at http://www.kuvendikosoves.org/common/docs/ligjet/2010-166-eng.pdf.

59. ITU Understanding Cybercrime, *supra* § 1 B, note 1, at 12.

60. UNODC Cybercrime Study *supra* § 1 C, note 7, at 11.

61. CIS Agreement provides that "offences against computer information" is defined as a criminal act of which target is computer information. *Supra* note 33, at Art. 1(a). *See also* Budapest Convention, *supra* § 1 B, note 32; AU Convention, *supra* note 48; and the Directive on Fighting Cyber Crime within Economic Community of West African States [hereafter, "ECOWAS Directive"], at https://ccdcoe.org/sites/default/files/documents/ECOWAS-110819-FightingCybercrime.pdf.

62. *See* SCO, Agreement between the Governments of the Member States of the SCO on Cooperation in the Field of International Information Security (2009) [hereafter, "SCO Agreement"], Art. 2., at http://www.ccdcoe.org/sites/default/files/documents/SCO-090616-IISAgreement.pdf (considering "information crime" as one of the major threats in the field of ensuring international information security); Annex 1, *ibid.* (stating that "information crime" means use of and/or attack on information resources in the information space for illegal purposes).

63. CIS Agreement, *supra* note 47.

64. *See* SCO Agreement, *supra* note 62.

65. OAS provides that "For the purposes of this diagnosis, 'cybercrime' is defined as a criminal activity in which information technology systems (including, *inter alia,* telecommunications and computer systems) are the corpus delicti or means of committing an offense." Final Report of the Second Meeting of Government Experts on Cyber Crime, (2000), OAS, p. 2, at http://www.oas.org/juridico/english/cybGE_IIrep.pdf *(in English). See also* Thomas Weigend, Preparatory Colloquium for the 20th International Congress of Penal Law on "Information Society and Penal Law" (organized by AIDP), § I (Criminal Law, General Part), § 1: Concept paper and questionnaire, (2012), AIDP, p. 1 (articulating that "The term 'cybercrime' is understood to cover criminal conduct that affects interests associated with the use of *information and communication technology (ICT)* (emphasis added) [….]. The common denominator and characteristic feature of all cybercrime offences and cybercrime investigation can be found in their relation to *computer systems, computer networks and computer data (emphasis added)* [….]"), at http://www.penal.org/IMG/pdf/Section_I_EN.pdf.

66. David Wall, "Cybercrimes: New Wine, No Bottles?," in Pamela Davies, Peter Francis & Victor Jupp (eds.), *Invisible Crimes: Their Victims and their Regulation,* (New York: Macmillan, 1999). *See also* Peter N. Grabosky, "Virtual Criminality: Old Wine in New Bottles?," Social & Legal Studies, Vol. 10 (2001), p. 243 (adapting the phrase be more of a matter of "old wine in new bottles"). The origin of the phrase is Biblical: "No one sews a piece of unshrunk cloth on an old cloak, for the patch pulls away from the cloak, and a worse tear is made. Neither is new wine put into old wineskins; otherwise, the skins burst, and the wine is spilled, and the skins are destroyed; but new wine is put into fresh wineskins, and so both are preserved." *The Bible,* Mat. 9:16–17 (NRSV).

67. Ian Walden, *Computer Crimes and Digital Investigations* (2d ed.), (Oxford: Oxford University Press, 2016), para. 2.27.

68. Anne Flanagan, "The Law and Computer Crime: Reading the Script of Reform," International Journal of Law & Information Technology, Vol. 13, Issue1 (2005), pp. 98–117.

69. For instance, it has been noted at UNICRI proceedings that "Due to the rapidly evolving nature of cybercrime, many governments and international organizations have shied away from adhering to a strict definition of the term." UNICRI, "Cyber Crime: Risks for the Economy and Enterprises": Proceedings of UNICRI roundtable, (29 Nov. 2013), p. 7, at http://www.unicri.it/in_focus/on/Cybercrime_Lucca.

70. UNODC Cybercrime Study, *supra* § 1 B, note 7, at 14–15.

71. For additional information, Policing Cybercrimes: Situating the Public Police in Networks of Security within Cyberspace, *supra* § 1 B, note 30, at 183–205, and Weigend, *supra* note 65.

72. *See* "Secretariat," United Nations, at http://www.un.org/en/sections/about-un/secretariat/index.html.

73. UN Secretariat, "Comprehensive and balanced approaches to prevent and adequately respond to new and emerging forms of transnational crime Working paper," (27 Jan. 2015) A/CONF.222/8, 13th UN Congress on Crime Prevention and Criminal Justice, at http://www.unodc.org/documents/congress//Documentation/A-CONF.222-8/ACONF222_8_e_V1500538.pdf.

74. UN Secretariat, *supra* note 3, at 6.

75. *See* "Commonwealth Secretariat," The Commonwealth, at http://www.commonwealthofnations.org/commonwealth/commonwealth-secretariat/.

76. *See* "About Us," The Commonwealth at http://thecommonwealth.org/about-us.

77. "Commonwealth Secretariat," *supra* note 75.

78. COMSEC, *supra* note 5.

79. *Ibid.*, at 11–12.

80. *Constitutive Act of the African Union*, (11 Jul. 2000), Lomé, Togo, CAB/LEG/23.15, Art. 2, at http://www.au.int/en/sites/default/files/ConstitutiveAct_EN.pdf.

81. *See* "AU in a Nutshell," African Union, at http://www.au.int/en/about/nutshell.

82. *Ibid.*

83. AU Convention, *supra* note 48. As with the other instruments covered in this section, the AU Convention is discussed as a means of illustrating the diverse ways that cybercrime has been classified. A deeper discussion of various international instruments can be found in § 5 B.

84. *Ibid.*, Ch. I: Electronic Transactions (Art. 2–7); Ch. II: Personal Data Protection (Art. 8–23); Ch. III: Promoting Cyber Security and Combating Cybercrime (Art. 24–38).

85. *Ibid.*, including the following offenses: (1) attacks on computer systems (Art. 29.1); (2) computerized data breaches (Art. 29.2); (3) content related offences (Art. 29.3); and (4) offences relating to electronic message security measures (Art. 29.4).

86. *Ibid.*, including the following offenses: (1) property offences (Art. 30.1); and (2) criminal liability for legal persons (Art. 30.2).

87. *Ibid.*, at Member States.

88. *Treaty of Economic Community of West African States* (ECOWAS), (28 May 1975), Lagos, Nigeria, at http://www.ecowas.int/ecowas-law/treaties/.

89. *See, e.g.*, "African Economic Community (AEC)," South African Dept. of International Relations and Cooperation, at http://www.dfa.gov.za/foreign/Multilateral/africa/aec.htm. *See also Abuja Treaty Establishing The African Economic Community*, (3 Jun. 1991), at http://www.wipo.int/edocs/lexdocs/treaties/en/aec/trt_aec.pdf.

90. ECOWAS Directive (2011), *supra* note 61.

91. Similarly, in criminalizing cybercrime, the AU Convention distinguishes between "offences specific to information and communication technologies" (Art. 29) and those "adapting certain offences to information and communication technologies" (Art. 30). *See* AU Convention, *supra* note 48.

92. Morris Odhiambo, Rudy Chitiga & Solomon Ebobrah, *The Civil Society Guide to Regional Economic Communities in Africa* (Oxford: African Books Collective Limited, 2016), p. 57.

93. *See* "About UNODC," UNODC, at https://www.unodc.org/unodc/about-unodc/index.html?ref=menutop.

94. *See* UN General Assembly, *United Nations Millennium Declaration*, (8 Sep. 2000) A/RES/55/2, at http://www.un.org/millennium/declaration/ares552e.htm.

95. *See* "About UNODC," UNODC, *supra* note 93.

96. UNODC Cybercrime Study, *supra* § 1 B, note 7.

97. *Ibid.*, at 16.

98. UNICRI, "Cybercrime: Risks for the Economy and Enterprises," at http://www.unicri.it/in_focus/on/Cybercrime_Lucca.

99. *See* Michele Socco, "European Commission, Fight against Cybercrime: A European perspective," presented at the UNICRI roundtable on "Cybercrime and the risks for economy and enterprises" (2013).

100. *See* "Our Member States," CoE, at http://www.coe.int/en/web/about-us/our-member-states.

101. *Statute of the Council of Europe* (5 May 1949), ETS No. 1 [hereafter, "Treaty of London"], Art. 1(a), at http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/001.

102. *Ibid. See also* "About Us," CoE, at https://www.coe.int/web/about-us/who-we-are.

103. *See* "Conventions," CoE, at http://www.coe.int/en/web/conventions/. Conventions and agreements opened for signature between 1949 and 2003 were published in the "European Treaty Series" (ETS No. 1 to 193 included). Since 2004, this Series is continued by the "Council of Europe Treaty Series" (CETS No. 194 and following). *Ibid.*

104. UNODC Cybercrime Study, *supra* § 1 B, note 7.

105. *Ibid.*

106. *See* "Summary," Details of ETS No. 185, at https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

107. UNODC Cybercrime Study, *supra* § 1 B, note 7, including the following offenses: (1) illegal access (Art. 2); (2) illegal interception (Art. 3); (3) data interference (Art. 4); (4) system interference (Art. 5); and (5) misuse of devices (Art. 6).

108. *Ibid.*, including the following offenses: (1) computer-related forgery (Art. 7); and (2) Computer-related fraud (Art. 8).

109. *Ibid.*, at Art.9.

110. *Ibid.*, at Art.10.

111. *Ibid.*, at Art.12.

112. *Ibid.*, at Art.13.

113. UNODC Conference Paper, *supra* note 2, at 5.

114. AU Convention, *supra* note 48.

115. ECOWAS Directive, *supra* note 44.

116. COMSEC, *supra* note 5, at http://thecommonwealth.org/media/news/communique-commonwealth-law-ministers-meeting-2014.

Referenced in: § B. Criminalized Conduct

1. *See supra* § 2 A.
2. *But see* Wall, *supra* § 1 B, note 33, at 6 (noting that "[t]here is global agreement in attitudes and rules condemning the distribution of child pornography").
3. *See, e.g.,* ITU Understanding Cybercrime, *supra* § 1 B, note 1, which provides, "[t]here is much lack of agreement regarding the content of material and to what degree specific acts should be criminalized."
4. For instance, the Budapest Convention makes hacking (termed "illegal access") the very first substantive crime. Budapest Convention, *supra* § 1 B, note 32, Art. 2. *See also* ITU Understanding Cybercrime, *supra* § 1 B, note 1.
5. *See supra* § 2 B, box 2.2.
6. *See, e.g.,* David Bisson, "5 Social Engineering Attacks to Watch Out for," Tripwire, (23 Mar. 2014), at https://www.tripwire.com/state-of-security/security-awareness/5-social-engineering-attacks-to-watch-out-for/.
7. *See, e.g.,* "Injection Attacks," Phpsecurity, at http://phpsecurity.readthedocs.io/en/latest/Injection-Attacks.html; "SQL Injection," Acunetix, at http://www.acunetix.com/websitesecurity/sql-injection/.
8. Vick Hargrave, "Hacker, Hacktivist or CyberCriminal?," Trend Micro Simply Security, (17 Jun 2012), at http://blog.trendmicro.com/whats-the-difference-between-a-hacker-and-a-cybercriminal/.
9. Stephanie Koons, "Researchers Examine Role of 'White Hat' Hackers in Cyber Warfare," Penn State News, (21 Jan. 2015), at http://news.psu.edu/story/341564/2015/01/21/research/ist-researchers-examine-role-%E2%80%98white-hat%E2%80%99-hackers-cyber-warfare.
10. Budapest Convention, *supra* § 1 B, note 32, at Art. 2. *See generally, ibid.*
11. *Ibid.*
12. Weigend, *supra* § 1 B, note 25, at 55.
13. The principle is captured by the Latin dictum *"actus reus non facit reum nisi mens sit rea"* ("the act is not culpable unless the mind is guilty"). *See, e.g.,* Oxford Reference Dictionary.
14. Budapest Convention, *supra* § 1 B, note 32.
15. *United States v. Marcel Lehel Lazar,* (E.D. Va. 2016). *See also* US Dept. of Justice "Romanian Hacker 'Guccifer' Pleads Guilty to Computer Hacking Crimes," US Attorney's Office, E.D. Va., (25 May 2016), at https://www.justice.gov/usao-edva/pr/romanian-hacker-guccifer-pleads-guilty-computer-hacking-crimes.
16. Pete Williams, "Guccifer, Hacker Who Says He Breached Clinton Server, Pleads Guilty," NBC News, (25 May 2016), at http://www.nbcnews.com/news/us-news/guccifer-hacker-who-says-he-breached-clinton-server-pleads-guilty-n580186.
17. Budapest Convention, *supra* § 1 B, note 32.
18. US Dept. of Justice, *supra* note 15.
19. Budapest Convention, *supra* § 1 B, note 32.
20. "Monitoring" is an ambiguous term internationally; some jurisdictions use it to mean taking content, while others use it to mean tracing.
21. Sarb Sembhi, "How to Defend Against Data Integrity Attacks," Computer Weekly, (Feb. 2009), at http://www.computerweekly.com/opinion/How-to-defend-against-data-integrity-attacks.
22. *See, e.g.,* "Edward Snowden: Leaks that Exposed US Spy Programme," BBC News, (17 Jan. 2014), at http://www.bbc.com/news/world-us-canada-23123964.
23. *See, e.g.,* "Snowden Designs Phone Case to Spot Hack Attacks," BBC News, (22 Jul. 2016), at http://www.bbc.com/news/technology-36865209.
24. Bunnie Huang, "Against the Law: Countering Lawful Abuses of Digital Surveillance," PubPub, (26 Jul. 2016), at https://www.pubpub.org/pub/direct-radio-introspection.
25. *See, e.g.,* Gordon Corera, "CIA Taps Huge Potential of Digital Technology," BBC News, (29 Jun. 2016), at http://www.bbc.com/news/world-us-canada-36462056.
26. *See, e.g.,* Kevin M. Gallagher, "Private Spies Deserve More Scrutiny," Huffington Post, (18 Jun. 2014), at http://www.huffingtonpost.com/kevin-m-gallagher/private-sector-surveillance_b_5171750.html.
27. *See, e.g.,* Laboratory of Cryptography and System Security (CrySyS Lab), "sKyWIper (a.k.a. Flame a.k.a. Flamer): A Complex Malware for Targeted Attacks," Budapest University of Technology and Economics, (31 May 2012), at https://www.crysys.hu/skywiper/skywiper.pdf.
28. David Kushner, "The Real Story of Stuxnet How Kaspersky Lab Tracked Down the Malware That Stymied Iran's Nuclear-Fuel Enrichment Program," IEEE Spectrum, (26 Feb. 2013), at http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet.
29. Gallagher, *supra* note 26.
30. CrysSyS Lab, *supra* note 27.
31. *See supra* § 2 B, box 2.4.
32. Gallagher, *supra* note 26.
33. CrysSyS Lab, *supra* note 27.
34. *Ibid.*
35. *Ibid.*
36. *See, e.g.,* "Data Diddling," Cyber Crime and Forensics Blog, at http://cybercrimeandforensic.blogspot.com/2009/02/data-diddling.html.
37. US Dept. of Justice, National Institute of Justice, Office of Justice Program, *Computer Crime: Criminal Justice Resource Manual* (2d ed.), OJP-86-C-002 (Aug. 1989).
38. *See, e.g., supra* § 1 B, case 1.3.
39. *See, e.g.,* Massimo Calabresi, "Election Hackers Altered Voter Rolls, Stole Private Data, Officials Say," Time, (22 Jun. 2017), at http://time.com/4828306/russian-hacking-election-widespread-private-data/.
40. *See, e.g.,* PM, "Could a New Case Stop Your Phone from Being Hacked?," BBC News, (22 Jul. 2016), at http://www.bbc.co.uk/programmes/p0428n3p.
41. *But see,* France's *Légifrance, le service public de l'accès au droit,* which, in addition to making publically available all sorts of basic legal documents (constitution, laws, regulations, court decisions, etc.), verifies the authenticity of the information published with each download.

42. *See, e.g.,* Hans A. von Spakovsky, "The Dangers of Internet Voting," The Heritage Foundation, at http://www.heritage.org/research/reports/2015/07/the-dangers-of-internet-voting; Michael Agresta, "Will the Next Election Be Hacked?," Wall Street Journal, (17 Aug. 2012), at http://www.wsj.com/articles/SB10000872396390444508504577595280674870186. *But see, e.g.,* Nicole Kobie, "Why Electronic Voting Isn't Secure – but May Be Safe Enough," Guardian, (30 Mar. 2015), at https://www.theguardian.com/technology/2015/mar/30/why-electronic-voting-is-not-secure.

43. *People v. Ressin,* No. 1978CR9793, Colo. Super. Ct. (Denver Dt.). For a broader position situating this crime in the time and in its context, *see* Jay Becker, "The Trial of a Computer Crime," Computer Law Journal. Vol. 2 (1980), p. 441, at http://repository.jmls.edu/cgi/viewcontent.cgi?article=1610&context=jitpl.

44. *See supra* § 1 B.

45. Viano, § 1 B, note 39.

46. Terry Chia, "Confidentiality, Integrity and Availability (CIA): The Three Components of the CIA Triad," IT Security Community Blog, (20 Aug. 2012), at http://security.blogoverflow.com/2012/08/confidentiality-integrity-availability-the-three-components-of-the-cia-triad/.

47. One form of cybersabotage technique is cyber-bombing, wherein in malicious code, often called a "logic bomb" or "slag code", is programmed to execute under certain circumstances, such upon failure to appropriately respond to a program command, or after the lapsing of a certain period of time. Such a technique is common in cyberwar and/or cyberterrorism. *See, e.g.,* Sct'y. Carter & Gen. Dunford, US Dept. of Defense Press Briefing, Pentagon Briefing Room, (29 Feb. 2016), at http://www.defense.gov/News/News-Transcripts/Transcript-View/Article/682341/department-of-defense-press-briefing-by-secretary-carter-and-gen-dunford-in-the. Those topics are beyond the scope of the Toolkit. Nonetheless, it bears noting that the lines between acts of cybercrime and cyberwar or cyberterrorism are increasingly blurred, especially, as the World Development Report has noted, "acts that might previously have been considered civilian attacks are now being uncovered as acts of states against states via nonstate actor proxies". *See* WDR, *supra* § 1 A, note 10.

48. Weigend, *supra* § 1 B, note 26, at 54.

49. As already noted, some acts that might otherwise constitute cybercrime, or that with the passage of time are revealed to be acts of states against states, and that might be characterized as cyberterrorism or cyberwarfare, are beyond the scope of this Toolkit. *See* WDR, *supra* § 1 A, note 10, at 222 *et seq.*

50. Andrea Peterson, "The Sony Pictures Hack, Explained," Washington Post, (18 Dec. 2014), at https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/.

51. *Ibid.*

52. *See, e.g.,* Aisha Harris, "Sony Really Should Release The Interview Online, and Soon," Slate, (17 Dec. 2014), at http://www.slate.com/blogs/browbeat/2014/12/17/the_interview_pulled_from_theaters_due_to_north_korea_s_apparent_data_hack.html.

53. David E. Sanger & Nicole Perlroth, "US Said to Find North Korea Ordered Cyberattack on Sony," New York Times, (17 Dec. 2014), at http://www.nytimes.com/2014/12/18/world/asia/us-links-north-korea-to-sony-hacking.html?_r=1.

54. *See infra* § 4 B.

55. Accepted freedom of expression restrictions range from child pornography, direct and public indictment, the commitment of genocide, the dissemination of hate speech, and incitement to terrorism. *See, e.g.,* Promotion and Protection of the Right to Freedom of Opinion and Expression, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression to UN General Assembly, Frank La Rue, A/66/290 (10 Aug. 2011), pp. 8–13, at http://www.ohchr.org/Documents/Issues/Opinion/A.66.290.pdf.

56. *See, e.g.,* ITU Understanding Cybercrime, *supra* § 1 B, note 1, at 21.

57. *Cf.* Jamaica: Child Pornography (Prevention) Act, § 5 (Processing or accessing child pornography), at http://moj.gov.jm/sites/default/files/laws/Child%20Pornograph%20%28Prevention%29%20Act.pdf.

58. *See, e.g.,* China rendered a judicial interpretation whose provisions allow application of pre-existing legislative provisions on traditional form of obscenity offences (Art. 363(1)1 & Art. 364(1)1 of the Criminal Law) to cover criminal behaviors involving obscene electronic information concretely depicting sexual acts by minors under 18 years of age. For details, *see* (1) China: Criminal Law, and (2) China: Interpretation of Some Questions on Concretely Applicable Law in the Handling of Criminal Cases of Using the Internet or Mobile Communication Terminals and Voicemail Platforms to Produce, Reproduce, Publish, Sell (also translated as "Peddle") or Disseminate Obscene Electronic Information (Sept. 2004), at https://chinacopyrightandmedia.wordpress.com/2004/09/09/interpretation-of-some-questions-on-concretely-applicable-law-in-handling-criminal-cases-of-using-the-internet-or-mobile-communication-terminals-and-voicemail-platforms-to-produce-reproduce-publish-2/#more-1700.

59. *See, e.g.,* Kosovo: Law on Prevention and Fight of the Cyber Crime (11 Mar. 2010), Art. 16 (Child pornography through computer systems), at http://mzhe.rks-gov.net/repository/docs/LIGJIPERPARANDALIMINDHE_LUFTIMINE_KRIMITKIBERNETIKE2010166-alb2010-166-eng.pdf; India: Information Technology (Amendment) Act, (2008), § 67B (Punishment for publishing or transmitting of material depicting children in sexual explicit act, etc., in electronic form) which was inserted into the Information Technology Act, (2000), at https://cc.tifrh.res.in/webdata/documents/events/facilities/IT_act_2008.pdf.

60. *See, e.g.,* "Argentina, Penal Code (as amended by Act No. 26388 of 2008), Article 128" (*in English*)," from: UN Committee on the Rights of the Child, "Consideration of Reports Submitted by States Parties under Art. 12, para. 1, of the Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography: Argentina," (10 Mar. 2010) CRC/C/OPSC/ARG/1, at pp. 18–19, at http://www.refworld.org/pdfid/50b3526a2.pdf.

61. *See, e.g.*, Brunei Darussalam: Penal Code (Amendment) Order, (2012), which inserted §§ 293A (Possession of Indecent Photograph of Child), 293B (Taking, Distribution, Showing, Advertisement and Access of Indecent Photograph of Child), 293C (Interpretation of §§ 293A and 293B), and 293D (Defense) into the Penal Code, at http://www.agc.gov.bn/AGC%20Images/LAWS/Gazette_PDF/2012/EN/S026.pdf.

62. "Cyberstalking, a New Crime: Evaluating the Effectiveness of Current State and Federal Laws," Missouri Law Review, Vol. 72 (2007), p. 125, at http://scholarship.law.missouri.edu/cgi/viewcontent.cgi?article=3985&context=mlr.

63. *See, e.g.*, US Dept. of Justice, National Institute of Justice, "Domestic Violence, Stalking, and Antistalking Legislation: An Annual Report to Congress under the Violence Against Women Act," (Apr. 1996), p. 1, at https://www.fas.org/sgp/crs/misc/R42499.pdf. Lisa N. Sacco, "The Violence Against Women Act: Overview, Legislation, and Federal Funding," US Congressional Research Service (CRS) (26 May 2015), at https://www.fas.org/sgp/crs/misc/R42499.pdf.

64. *See* US Dept. of Justice, National Center for Victims of Crime, *Problem-Oriented Guides for Police Problem-Specific Guides Series Guide: Stalking*, No. 22 (5 Jan. 2004), at https://victimsofcrime.org/docs/src/stalking-problem-oriented-policiing-guide.pdf?sfvrsn=0.

65. Katrina Baum, Shannan Catalano, Michael Rand & Kristina Rose, "Stalking Victimization in the United States," US Dept. of Justice, Office of Justice Programs, Bureau of Justice Statistics Special Report, (Jan. 2009) at https://www.justice.gov/sites/default/files/ovw/legacy/2012/08/15/bjs-stalking-rpt.pdf.

66. *Supra* note 60.

67. Paul Mullen, Michele Pathé & Rosemary Purcell, "Cyberstalking," Stalking Risk Profile, at https://www.stalkingriskprofile.com/victim-support/impact-of-stalking-on-victims.

68. *Ibid.*

69. *Leandra Ramm v. Colin Mak Yew Loong,* NRIC No. S7524695A (20 Dec. 2013).

70. Katharine Quarmby, "How the Law Is Standing Up to Cyberstalking," Newsweek, (13 Aug. 2014), at http://www.newsweek.com/2014/08/22/how-law-standing-cyberstalking-264251.html.

71. Claire Huang Jingyi, "3 Years' Jail, S$5,000 Fine for Man Who Harassed US Singer," TodayOnline, (21 Dec. 2013), at http://www.todayonline.com/singapore/3-years-jail-s5000-fine-man-who-harassed-us-singer?page=1.

72. Mark Albertson, "Singapore Cyberstalker Convicted, but Others Roam Free," Examiner, (6 Dec. 2013), at http://www.examiner.com/article/singapore-cyberstalker-convicted-but-others-roam-free.

73. *See* Protection from Harassment Act (Ch. 256A). *See also* Mong Palatino, "Singapore Criminalizes Cyber Bullying and Stalking," Diplomat, (24 Mar. 2014), at http://thediplomat.com/2014/03/singapore-criminalizes-cyber-bullying-and-stalking/.

74. EU Agency for Fundamental Rights, "Violence Against Women: An EU-wide Survey" (Mar. 2014), at http://fra.europa.eu/en/publication/2014/violence-against-women-eu-wide-survey-main-results-report.

75. *See* CoE, *Convention on Preventing and Combating Violence Against Women and Domestic Violence*, (11 May 2011) CETS No. 210, [hereafter, "Istanbul Convention"], at http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/210. However, cyberstalking is not listed as a punishable offense in the Budapest Convention. *Ibid.*

76. California led the way, becoming, in 1990, the first jurisdiction to specifically criminalize stalking in response to the murder of the television star Rebecca Schaeffer. *See, e.g.*, Berkman Center for Internet & Society, "State and Federal Stalking Laws," Harvard University, at https://cyber.law.harvard.edu/vaw00/cyberstalking_laws.html.

77. *See* "Factsheet: The Violence Against Women Act," The White House of President Obama, at https://www.nvcc.edu/support/_files/Violence-Against-Women-Act-Fact-Sheet.pdf.

78. California also became the first state to specifically criminalize cyberstalking. *See* Naomi Harlin Goodno, "Cyberstalking, a New Crime: Evaluating the Effectiveness of Current State and Federal Laws," Missouri Law Review (2007), at http://scholarship.law.missouri.edu/cgi/viewcontent.cgi?article=3985&context=mlr.

79. The added language criminalized the "use [of…] any interactive computer service or electronic communication service or electronic communication system of interstate commerce". USC Title 18, § 2261A - Stalking, at https://www.law.cornell.edu/uscode/text/18/2261A. The most recent reauthorization was signed into law in 2013. *See* "1 is 2 Many:, Resources Violence Against Women Act," The White House of President Barack Obama, at https://www.whitehouse.gov/1is2many/resources.

80. While all fifty states, the District of Columbia and US Territories have criminalized stalking, cyberstalking has only been specifically addressed by some thirty-five jurisdictions. *See, e.g.*, Working to Halt Online Abuse, at http://www.haltabuse.org/resources/laws/; "Stalking Technology Outpaces State Laws," National Center for Victims of Crime, at https://victimsofcrime.org/docs/src/stalking-technology-outpaces-state-laws17A308005D0C.pdf?sfvrsn=2. This fact is troubling as the constitutional limits on US federal law mean that VAWA does not apply to cyberstalking conducted exclusively within the jurisdiction of any one state or territory and must involve the interstate or foreign commerce. *See* USC TItle 18, § 2261A(1)- Stalking, at https://www.law.cornell.edu/uscode/text/18/2261A. That much said, the inherently cross-border nature of electronic communications makes it is likely that US federal law would be applicable. Moreover, courts have facilitated legislative hiccups by extending existing, traditional statutes to include electronic tools. *See, e.g., Colorado v. Sullivan*, 53 P.3d 1181 (Colo. Ct. App. 2002).

81. Katrina Baum, Shannan Catalano, Michael Rand & Kristina Rose, "National Crime Victimization Survey Stalking Victimization in the United States," US Dept. of Justice, Bureau of Justice Statistics Special Report (Jan. 2009), p. 3, at https://www.justice.gov/sites/default/files/ovw/legacy/2012/08/15/bjs-stalking-rpt.pdf.

82. *See, e.g., Colorado v. Sullivan, supra* note 77 (where a Colorado court ruled that the phrase "under surveillance" in the state's stalking law included electronic surveillance and that a Colorado man's installation of a GPS device in his estranged wife's car to check on her whereabouts during their divorce proceedings constituted stalking).

83. *United States v. Jake Baker,* 104 F.3d 1492 (6th Cir. 1997).

84. *Elonis v. United States,* 575 U.S. (2015).

85. *See, e.g.,* "Building Your Case," End Stalking in America, Inc., at http://www.esia.net/Building_your_Case.htm.

86. *See* "Stalking Technology Outpaces State Laws," *supra* note 77, at https://victimsofcrime.org/docs/src/stalking-technology-outpaces-state-laws17A308005D0C.pdf?sfvrsn=2.

87. Quoted in Katharine Quarmby, *supra* note 70.

88. Martin Evans, "Fraud and Cyber Crime are Now the Country's Most Common Offences," Telegraph, (19 Jan. 2017), at http://www.telegraph.co.uk/news/2017/01/19/fraud-cyber-crime-now-countrys-common-offences/.

89. PricewaterhouseCoopers, *PWC's 2014 Global Economic Crime Survey: Economic Crime, A Threat to Business Globally* (2014) [hereafter, "PWC 2014 Global Economic Crime Survey"], at https://www.pwc.at/publikationen/global-economic-crime-survey-2014.pdf.

90. Gordon M. Snow, Statement before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit, (Washington: FBI, 2011), at https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector

91. *See* PWC 2014 Global Economic Crime Survey, *supra* note 89.

92. Albin Krebs, "Willie Sutton Is Dead at 79," New York Times, (19 Nov. 1980). Although lore would have it that Sutton said it in response, Sutton himself denies having actually made the statement, writing that, "The credit belongs to some enterprising reporter who apparently felt a need to fill out his copy. I can't even remember when I first read it. It just seemed to appear one day, and then it was everywhere. If anybody had asked me, I'd have probably said it[…] it couldn't be more obvious." Willie Sutton with Edward Linn, *Where the Money Was: The Memoirs of a Bank Robber,* (New York: Crown/Archetype, 2004).

93. Andrew M. Cuomo & Benjamin M. Lawsky, "Report on Cyber Security in the Banking Sector," New York State Dept. of Financial Services, (New York: New York State Dept. of Financial Services, 2014), at http://www.dfs.ny.gov/reportpub/dfs_cyber_banking_report_052014.pdf.

94. A.R. Raghavan & Latha Parthiban, "The Effect of Cybercrime on a Bank's Finances," International Journal of Current Research and Academic Review, Vol. 2, No. 2, (Feb. 2014), pp. 173–78, at http://www.ijcrar.com/vol-2-2/A.R.%20Raghavan%20and%20Latha%20Parthiban.pdf.

95. Lucian Constantin, "Target Point-of-Sale Terminals Were Infected with Malware," PC World, (13 Jan. 2014), at http://www.pcworld.com/article/2087240/target-pointofsale-terminals-were-infected-with-malware.html.

96. *See, e.g.,* The 2014 Symantec Internet Security Threat Report, Symantec, (Mar. 2014), at http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf. *See also,* Kamala Harris, the 2014 California Data Breach Report, California Office of the Attorney General, (Oct. 2014), at https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/2014data_breach_rpt.pdf.

97. "Business Email Compromise, Public Service Announcement," Internet Crime Complaint Center & Federal Bureau of Investigation, (2015), at https://www.ic3.gov/media/2015/150122.aspx; Brian Krebs, "FBI: Businesses Lost $215M to Email Scams," Krebs on Security, (2015), at http://krebsonsecurity.com/2015/01/fbi-businesses-lost-215m-to-email-scams/.

98. *See supra* § 2 B, box 2.2.

99. "Anonymous Hacktivists Say Wikileaks War to Continue," BBC News, (9 Dec. 2010), at http://www.bbc.com/news/technology-11935539.

100. David Carlisle, "Virtual Currencies and Financial Crimes," RUSI Occasional Paper, Royal United Services Institute for Defence and Security Studies (RUSI), (March 2017), at https://rusi.org/sites/default/files/rusi_op_virtual_currencies_and_financial_crime.pdf

101. *Ibid.*

102. USC Title 18, § 1343 "Fraud by Wire, Radio, or Television." *See also United States v. Cassiere,* 4 F.3d 1006 (1st Cir. 1993); *United States v. Ames Sintering Co.,* 927 F.2d 232 (6th Cir. 1990).

103. "Net Losses: Estimating the Global Cost of Cybercrime," McAfee & CSIS, (June 2014), at http://csis.org/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf.

104. *Ibid.*

105. *United States v. Drinkman, Kalinin, Rytikov, Smilianets, & Rytikov* (Criminal No. 09-626 (JBS) (S-2)).

106. Indictment: *United States v. Vladimir Drinkman, Aleksandr Kalinin, Roman Kotov, Mikhail Rytikov, and Dmitriy Smilianets,* (D.N.J. 2009), at http://www.justice.gov/iso/opa/resources/518201372511217608630.pdf.

107. *United States v Drinkman, Kalinin, Kotov, Rytikov, Smilianets,* UNODC Cybercrime Repository, at https://www.unodc.org/cld/case-law-doc/cybercrimecrimetype/usa/us_v_drinkman_kalinin_kotov_rytikov_smilianets.html?&tmpl=cyb.

108. Targeted institutions included, among others, Heartland Payment Systems Inc., Euronet, Global Payment Systems, 7-Eleven, Carrefour S.A., JC Penney Inc., Hannaford Brothers Co., Wet Seal Inc., Commidea Ltd., JetBlue Airways, Visa Inc., Diners, Ingenicard US, Inc., NASDAQ, Dow Jones Inc., 'Bank A' (a major UAE bank), and Dexia Bank Belgium.

109. Report on Cyber Security in the Banking Sector, *supra* note 99.

110. Paula Rosenblum, "In the Wake of Target Data Breach," Forbes, (17 Mar. 2014), at http://www.forbes.com/sites/paularosenblum/2014/03/17/in-wake-of-target-data-breach-cash-becoming-king-again/.

111. *United States v. Ross William Ulbricht,* 79 F.Supp. 3d 466 (S.D.N.Y. 2015). Silk Road was tried under a number of legal theories including US banking, narcotics trafficking, criminal conspiracy and "cybercrime". Ulbricht's appeal of his conviction on the grounds of corruption of DEA agents interfering with evidence and other procedural issues at trial was denied in May 2017, *see United States v. Ulbricht,* No. 15-1815, (2d Cir. 2017), at https://cases.justia.com/federal/appellate-courts/ca2/15-1815/205494850/0.pdf?ts=1496418409. This case is highlighted again further on as an example of the procedural aspects surrounding search and seizure. *See infra* § 4 A, case 4.1.

112. *Ibid.* As noted, the Silk Road case is highlighted in the Toolkit for a number of reasons. *Ibid.* More generally, it bears noting that "dark web" markets—where drugs, weapons, malware, toxic chemicals, stolen data and the like are traded—is unlikely to go away. Rather, as cyberspace continues to gain both commercial and social importance, the place for such dark markets is only likely to grow. Indeed, by all indications, that growth is very substantial: recently, two additional dark web marketplaces—AlphaBay and Hansa—were shut down by FBI-led, global police efforts. *See* Chris Baraniuk, "AlphaBay and Hansa Dark Web Markets Shut Down," BBC News, (20 Jul. 2017), at http://www.bbc.com/news/technology-40670010. In terms of both traffic and value, AlphaBay and Hansa dwarfed Silk Road: while Silk Road only had 14,000 listings for illicit items of various kinds when it was seized in 2013, the DoJ said that AlphaBay had more than 350,000 listings, with US$450m was spent via the marketplace between May 2015 and February 2017. *Ibid.* While the impact of shutting down AlphaBay and Hansa is unclear, there are indications that trade on several of the other dark web's illegal markets has increased, though the sales of some goods appear to have been reduced. *See, e.g.,* Leo Kelion, "Dark Web Markets Boom after Alphas Bay and Hansa busts," BBC News, (1 Aug. 2017), at http://www.bbc.com/news/technology-40788266. The growing dark side of cyberspace is a matter with which society at large will—constructively and collectively—have to grapple; fighting cybercrime and assuring cybersecurity are central elements therein. *See, e.g.,* Ronald Deibert, "The Growing Dark Side of Cyberspace (… and What to Do About It)," Penn State Journal of Law & International Affairs, Vol. 1, Issue 2 (Nov. 2012), at http://elibrary.law.psu.edu/cgi/viewcontent.cgi?article=1012&context=jlia. For a provocative, fictional depiction of the role of cyber exchanges, *see* Jennifer Haley, "The Nether", *supra* § 1 B, note 7.

113. Tamara Tabo, "United States v. The Internet: America's Most Wanted May Look a Lot Like You," AbovetheLaw.com, (12 Jun. 2015), at http://abovethelaw.com/2015/06/united-states-v-the-internet-americas-most-wanted-may-look-a-lot-like-you/

114. *See, e.g.,* "How Blockchain Tech Could Change the Way We Do Business," BBC News, (22 Jan. 2016), at http://www.bbc.com/news/business-35370304.

115. *Ibid.*

116. *See* Don Tapscott & Alex Tapscott, "The Impact of the Blockchain Goes Beyond Financial Services," Harvard Business Review (10 May 2016), at https://hbr.org/2016/05/the-impact-of-the-blockchain-goes-beyond-financial-services ("where not just information but anything of value – money, titles, deeds, music, art, scientific discoveries, intellectual property, and even votes – can be moved and stored securely and privately. On the blockchain, trust is established, not by powerful intermediaries like banks, governments and technology companies, but through mass collaboration and clever code. Blockchains ensure integrity and trust between strangers. They make it difficult to cheat.").

117. *See, e.g.,* US Currency and Foreign Transactions Reporting Act of 1970 (*see* USC Title 18, §§ 5311–5330 and 31 CFR Chapter X [formerly 31 CFR Part 103] ("Bank Secrecy Act" or "BSA").

118. *Ibid.,* at para. 71.

119. *See, e.g.,* United Kingdom: Computer Misuse Act 1990, (criminalizing three acts: (1) Unauthorized access to computer material; (2) unauthorized access with intent to commit or facilitate commission of further offences; (3) unauthorized modification of computer material), at http://www.legislation.gov.uk/ukpga/1990/18/contents. It should be noted that amendments to the Computer Misuse Act were introduced in the Police and Justice Act 2006, http://www.legislation.gov.uk/ukpga/2006/48/part/5/crossheading/computer-misuse.

120. USC Title 18, § 1030(a)(6)(A) & (B)

121. *Ibid.,* at para. 81.

122. A review of the global state of cybercrime legislation by the CoE found that only 70% of studied countries had legislation in place targeting the misuse of devices; dual use of devices was not considered, with focus being on the production of some specific devices; misuse of devices was found to be criminalized only in relation with illegal access or system interference. *See* Cristina Schulman, "The Global State of Cybercrime Legislation," Workshop 1: Cybercrime legislation (Strasbourg: Octopus Conference, 6–8 Jun. 2012), at https://rm.coe.int/16802f240b. *See also Geoffrey Andare v. Attorney General & 2 others,* [2016] eKLR, Petition No.149 of 2015, High Court of Kenya at Nairobi Milimani Law Courts, Constitutional and Human Rights Division, at http://kenyalaw.org/caselaw/cases/view/121033/.

123. EU Directive 2013/40/EU, at Art. 7.

124. For example, quantum computing is expected to both revolutionize computing and unravel modern encryption technology. *See supra* § 1 C, box 1.3.

125. *Andare, supra* note 122.

126. *See* Kenya: Information and Communications Act, Chapter 411A § 29, at https://www.unodc.org/res/cld/document/ken/1930/information-and-communications-act_html/Kenya_Information_and_Communications_Act_2_of_1998.pdf.

127. *Ibid.*

128. *Supra* note 114, (stating "the provisions of section 29 are so wide and vague that they offend the requirements with regard to law that carries penal consequences and do not meet the criteria set in Art. 24 of the Constitution which provides instances when rights can be limited), para. 80 & 99. Art.33(2), Constitution of Kenya, (2010), at https://www.kenyaembassy.com/pdfs/the%20constitution%20of%20kenya.pdf.

129. *Ibid.* (stating "Section 29 imposes a limitation on the freedom of expression in vague, imprecise and undefined terms […]").

130. *See supra* § 2 B, case 2.6. *See also infra* § 4 A, case 4.1.

Referenced in: § C. Procedural Issues

1. This section focuses on investigative and prosecutorial "procedural" issues; "due process" issues are treated in § 5 A, *infra*.

2. In practice, procedural issues are never entirely detached from the substantive specification of an offense. The specification of the elements and seriousness of the offense are important in determining whether cognizance it taken of a suspected violation, and, if so, what level of intrusiveness will be permitted during investigation.

3. *See, e.g.*, Budapest Explanatory Report, *supra* § 1 D, note 14, at para. 132 ("Not only must substantive criminal law keep abreast of these new abuses, but so must criminal procedural law and investigative techniques").

4. Tonya Putnam & David Elliot, *Chapter 2- International Responses to Cyber Crime*, (Stanford: Hoover Institution Press, 2001), pp. 1–2, at http://www.hoover.org/sites/default/files/uploads/documents/0817999825_35.pdf.

5. For instance, the offender is based in one or more different countries, the services utilized are in different countries, the technology protects is anonymous, the communications are encrypted.

6. Most tellingly, it bears emphasizing that e-evidence is information stored or transmitted in binary form ("0" and "1"), and that that binary code assigns a bit string to each symbol or instruction. Such being the case, the evidence is in many ways both illusionary and illusive: the "original" evidence can be identically copied with no difference between the two except the time of their existence, and its integrity can be very easily compromised. For deeper discussion, *see supra* § 2 B.

7. US Dept. of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* (Washington: Office of Legal Education, 2009) [hereafter, "Searching and Seizing e-Evidence"], at https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf; UNODC Cybercrime Study, *supra* § 1 C, note 7.

8. Thomas K. Clancy, *Cyber Crime and Digital Evidence: Materials and Cases* (New York: Lexisnexis, 2011); Cameron S. D. Brown, "Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice," International Journal of Cyber Criminology, Vol. 9, Issue1 (2015), Issue 55, pp. 66–67.

9. ITU Understanding Cybercrime, *supra* § 1 B, note 1, at 251–56.

10. *See, e.g.*, Budapest Explanatory Report, *supra* § 1 D, note 14, at para. 12 ("[T]here are some differences with respect to the search of computer data, which may necessitate different or special procedural provisions to ensure that computer data can be obtained in a manner that is equally effective as a search and seizure of tangible data. […] Some changes may be required to domestic law to ensure that intangible data can be searched and seized. […D]ue to the connectivity of computer systems, data may not be stored in the particular computer that is searched, but such data may be readily accessible to that system. […Allowing such searches may] require new laws to permit an extension of the search to where the data is actually stored (or the retrieval of the data from that site to the computer being searched), or the use traditional search powers in a more coordinated and expeditious manner at both locations."). *See, e.g.*, American Law Institute, "Model Code of Cybercrime Investigative Procedure," at http://www.crime-research.org/library/Model_Code.htm.

11. USC Title 18, §§ 3123 (1986).

12. USA PATRIOT Act, *supra* § 1 C, note 10.

13. *See supra* § 1 B.

14. Korea: Criminal Procedure Act, No. 12784 (15 Oct. 2014) [hereafter "Korean Criminal Procedure Act"], at http://elaw.klri.re.kr/eng_mobile/viewer.do?hseq=33081&type=sogan&key=9 (*in English*), Art. 106(3), ("Where the object to be seized is a computer disc or other data storage medium similar thereto […], the court shall require it should be submitted after the data therein are printed out or it is copied within the specified scope of the data stored: Provided, That the data storage medium or such may be seized, when it is deemed substantially impossible to print out or copy the specified scope of the data or deemed substantially impracticable to accomplish the purpose of seizure.").

15. Regarding the need for a formalization of computer forensics, *see* Ryan Leigland & Axel W. Krings, "A Formalization of Digital Forensics," International Journal of Digital Evidence, Vol. 3, Issue 2 (2004), p. 2.

16. Michell Lange & Kristin Nimsger, *Electronic Evidence and Discovery* (Chicago: Section of Science & Technology Law, American Bar Association, 2004), p. 6.

17. With regard to developments, *see* Danny Abramovitch, "A Brief History of Hard Drive Control," Control Systems Magazine, EEE, Vol. 22, Issue 3 (2002), p. 28 *et seq.;* Tom Coughlin, Dennis Waid, & Jim Porter, "The Disk Drive, 50 Years of Progress and Technology Innovation," Coughlin Associates, (2005), at www.tomcoughlin.com/Techpapers/DISK%20DRIVE%20HISTORY,%20TC%20Edits,%20050504.pdf.

18. Scott Giordano, "Electronic Evidence and the Law," Information Systems Frontiers, Vol. 6, No. 2 (2006), p. 161; Stephen Willinger & Robin Wilson, "Negotiating the Minefields of Electronic Discovery," Richmond Journal of Law & Technology, Vol. 10, Issue 5 (2004), at http://jolt.richmond.edu/v10i5/article52.pdf.

19. Malaga, "Requirements for the Admissibility in Court of Digital Evidence," in: Syllabus to the European Certificate on Cybercrime and E-Evidence, (2008), p. 208 *et seq.*

20. *See, e.g., Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, supra* note 7; US Dept. of Justice, Criminal Division, Office of Professional Development and Training, "Federal Guidelines for Searching and Seizing Computers," Bureau of National Affairs, Criminal Law Reporter, Vol. 56 (1994), p. 5, at https://epic.org/security/computer_search_guidelines.txt; Korean Constitution, Art.12(1) & 12(3); Korean Criminal Procedure Act, *supra* note 14, at Arts. 114 & 215. *See also infra* § 2 C, case 2.9.

21. In US law, contraband, an instrumentality of a crime or fruits of crime and therefore may be physically seized. *See* Rule 41, Federal Rules of Criminal Procedure, at https://www.law.cornell.edu/rules/frcrmp/rule_41. *See also* Giordano, *supra* note 18.

22. *Ibid.*

23. *Ibid.*, at 71.

24. *See, e.g., United States v. Huitt*, 2007 WL 2355782, at *4, (D. Idaho 2007).

25. Supreme Court of Korea, Order 2009Mo1190 (26 May 2011), at http://library.scourt.go.kr/SCLIB_data/decision/15-2009Mo1190.htm (*summary in English*).

26. *Ibid.* at para.2.

27. *Ibid.* at para.1.

28. *Ibid.*

29. *Ibid.*

30. Field tools include Cellebrite, UltraDock, EnCase Portable, etc. For more information, *see* "22 Popular Computer Forensics Tools," InfoSec Institute, at http://resources.infosecinstitute.com/computer-forensics-tools/.

31. Brown, *supra* note 8.

32. Gon Ruibin & Mathias Gaertner, "Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework," International Journal of Digital Evidence, Vol. 4, No. 1 (2005).

33. Giuseppe Vaciago, *Digital Evidence* (Torrino: Giappichelli, 2012), "Situation Report on the Admissibility of Electronic Evidence in Europe," (Ch. II.1), in: *Syllabus to the European Certificate on Cybercrime and E-Evidence,* (2008), p. 220.

34. *See Weeks v. United States*, 232 U.S. 383 (1914). *See also,* H. Frank Way, Jr., "Exclusion of Evidence Illegally Obtained," Tennessee Law Review, Vol. 26 (1959) (noting that this "rule […] holds that an individual, whose rights have been violated under the Fourth Amendment, can prohibit the introduction in a trial against him of any evidence seized as a result of the illegal search and seizure. The rule generally works through mechanics of a pre-trail motion for the exclusion and/or suppression of the illegally seized evidence.").

35. US Rules Enabling Act, USC Title 28, §§ 2072, 2074.

36. *US Federal Rules of Criminal Procedure (eff. 16 Dec. 2016),* Rule 41(e)(2)(B) (Warrant Seeking Electronically Stored Information), at http://www.uscourts.gov/rules-policies/current-rules-practice-procedure.

37. *Ibid.*

38. *United States v. Austin Ayers Winther,* (E.D. Pa. 2011), p. 21, at http://www.paed.uscourts.gov/documents/opinions/11d1281p.pdf (quoting the US Federal Rules of Criminal Procedure, *supra* note 36).

39. Supreme Court of Korea, Order 2011Do10508 (29 Mar. 2012), at http://www.law.go.kr/precInfoP.do?mode=0&evtNo=2011%EB%8F%8410508 (*in Korean*). *See also* UN Committee against Torture, "Consideration of reports submitted by States parties under article 19 of the Convention pursuant to the optional reporting procedure," Third to Fifth Periodic Reports of States Parties due in 2012, Korea, (29 Feb. 2016), at http://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2FPPRiCAqhKb7yhsvF6hiQLJAnpG6iplFwLNHHRo0OD78WS4LFAhS78ybK9cAdJ5ZfbR4liAXlyMG4l6gfS%2BNuCz6URY2YsRMgaSD1rC4Di8J1OSunD47yXd4UH.

40. UNODC Cybercrime Study, *supra* § 1 C, note 7, at 159.

41. *Ibid.*

42. Richard Nolan, Colin O'Sullivan, Jake Branson & Cal Waits, *First Responders Guide to Computer Forensics,* (Arlington, VA: SEI, 2005), p. 64, at https://resources.sei.cmu.edu/asset_files/Handbook/2005_002_001_14429.pdf.

43. Leigland & Krings, *supra* note 14, at 9.

44. *See* John Vacca, *Computer Forensics, Computer Crime Scene Investigation,* (2d ed.), (Hingham, MA: Charles River Media, 2005), p. 30.

45. Botnets is a short term for a group of compromised computers running programs that are under external control. For more details, *see* Clay Wilson, *Botnets, Cybercrime, and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress,* (Washington, DC: US Dept. of State, 2007), p. 4, www.fas.org/sgp/crs/terror/RL32114.pdf. *See also* collected resources, and links in the ITU Botnet Mitigation Toolkit, (2008), at www.itu.int/ITU-D/cyb/cybersecurity/projects/botnet.html.

46. Nolan *et al.*, *supra* note 42, at 29.

47. Lange & Nimsger, *supra* note 16.

48. Regarding the ability to manipulate the time information and the response in forensic investigations, *see* Pavel Gladyshev & Ahmed Patel, "Formalizing Event Time Bounding in Digital Investigations, International Journal of Digital Evidence," Vol. 4, No. 1 (2005); Regarding dynamic time analysis, *see* Michael C. Weil, "Dynamic Time & Date Stamp Analysis," International Journal of Digital Evidence, Vol. 1, Issue 2, (2002).

49. Eoghan Casey, *Digital Evidence and Computer Crime,* (London: Academic Press, 2004), p. 16.

50. Carole Chaski, "Who's at the Keyboard? Authorship Attribution in Digital Evidence Investigations," International Journal of Digital Evidence, Vol. 4, No. 1 (2005).

51. Brown, *supra* note 8.

52. For guidelines on how to carry out the seizure of computer equipment, *see, e.g., General Guidelines for Seizing Computers and Digital Evidence,* US State of Maryland, Maryland State Police, at https://www.coursehero.com/file/8005384/Article-Maryland-Seize-Computers-1/.

53. Lange & Nimsger, *supra* note 16, at 24.

54. Gladyshev & Patel, *supra* note 48, at 283 *et seq.*

55. The Toolkit uses the term "ISP" to include all electronic communications service providers, and not only internet service providers.

56. UNODC Cybercrime Study, *supra* § 1 C, note 7, at 144.

57. For an overview of the debate, *see* Marco Gercke, "The Role of Internet Service Providers in the Fight Against Child Pornography," Computer Law Review International, (2009), p. 65 *et seq.*

58. *See* Cormac Callanan & Marco Gercke, *Study on the Cooperation Between Service Providers and Law Enforcement Against Cybercrime: Towards Common Best-of-Breed Guidelines?,* (Strasbourg: CoE, 2008), at https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802f69a6.

59. John Leyden, "FBI Sought Approval to Use Spyware against Terror Suspects", Register, (8 Feb. 2008), at www.theregister.co.uk/2008/02/08/fbi_spyware_ploy_app/; Declan McCullagh, "FBI Remotely Installs Spyware to Trace Bomb Threat," CNet, (18 Jul. 2007), at https://www.cnet.com/news/fbi-remotely-installs-spyware-to-trace-bomb-threat/; Bogdan Popa, "FBI Fights against Terrorists with Computer Viruses," Softpedia, (19 Jul. 2007), at http://news.softpedia.com/news/FBI-Fights-Against-Terrorists-With-Computer-Viruses-60417.shtml.

60. Gaurav Gupta, Chandan Mazumdar, & M.S. Rao, "Digital Forensic Analysis of E-Mails: A Trusted E-Mail Protocol," International Journal of Digital Evidence, Vol. 2, No. 4 (2004).

61. For more information, *see* Larry Crumbley, Lester Heitger & Stevenson Smith, *Forensic and Investigative Accounting,* (2005), § 14.12; Michael Caloyannides, Privacy Protection and Computer Forensics, (2004), p. 149.

62. The term "phishing" describes an act that is carried out to make targets disclose personal/secret information. It originally described the use of emails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph" is linked to popular hacker naming conventions. *See* Marco Gercke, "The Criminalization of Phishing and Identity Theft," *Computer und Resht,* (2005), p. 606; Gunter Ollmann, "The Phishing Guide: Understanding & Preventing Phishing Attacks," IBM, (8 Jun. 2005), at http://pdf.textfiles.com/security/nisrphishing.pdf.

63. Gladyshev & Patel, *supra* note 48, at 19.

64. For more information, *see* Von Jens Todt, *Fahnder ueberpruefen erstmals alle deutschen Kreditkarten,* Spiegel Online, (8 Jan. 2007), at www.spiegel.de/panorama/justiz/0,1518,457844,00.html (*in German*).

65. Marc Goodman, "Why the Police Don't Care About Computer Crime," Harvard Journal of Law & Technology, Vol. 10, No. 3 (1997), p. 472.

66. "Is Bitcoin Turning into a Cyber Crime Currency?," Cyberoam, (6 Dec. 2012), at https://web.archive.org/web/20160404100125/http://www.cyberoam.com/blog/is-bitcoin-turning-into-a-cyber-crime-currency-2/ ("The trouble becomes obvious when creators of dreaded Zeus Botnet start using Bitcoins for transactions, the anonymous drug sites do brisk business through Bitcoins, hacktivists are quick to Tweet their gratitude on anonymous Bitcoin donation and Wikileaks openly proclaims acceptance of Bitcoin donation. So is the currency turning into a crime currency? The inherent structure of Bitcoin system is based on P2P network that lacks a central server making it very difficult to detect criminal transactions, discover the identity of users or acquire full transaction records of illicit money transfers. The security companies are forever racing against cybercrime in securing businesses and institutions. And in case of breaches, the security companies provide electronic trail, which the law applies to trace the activities in real world that finally nails them. By leveraging the decentralized Bitcoin system, criminals not only make it hard to trail electronically, but leave very few foot prints in the real world, making prosecution almost impossible."); *See also* Goodman, *supra* note 65.

67. *See, e.g.,* UNODC Cybercrime Study, *supra* § 1 C, note 7.

68. *Ibid.,* at xxv.

69. Searching and Seizing e-Evidence, *supra* note 7. For example, the United States Code does not require participation of a law enforcement officer in the scene when executing the search and seizure on the communication data stored by the service provider. For details, *see* USC Title 18, § 2703(g) - Presence of Officer Not Required, at http://stanford.edu/~jmayer/law696/week7/Stored%20Communications%20Act.pdf.

70. *Microsoft Corp. v. United States,* No. 14-2985 (2d Cir. 2016), at http://law.justia.com/cases/federal/appellate-courts/ca2/14-2985/14-2985-2016-07-14.html.

71. USC Title 18, §§ 2701–2712.

72. James C. Francis IV, Magistrate Judge, Memorandum and Order, *In the Matter of a Warrant to Search a Certain Email Account Controlled and Maintained by Microsoft Corporation,* (S.D.N.Y. 2014), at http://pdfserver.amlaw.com/nlj/microsoft-warrant-sdny.pdf; USC Title 18, § 2703 (a), *supra* note 64.

73. Loretta A. Preska, Chief US District Judge, Memorandum and Order, *In the Matter of a Warrant to Search a Certain Email Account Controlled and Maintained by Microsoft Corporation,* (S.D.N.Y. 2014), at http://online.wsj.com/public/resources/documents/microsoftstay.pdf.

Referenced in: § D. Evidentiary Issues

1. Latin: "The burden of proof is on the one who declares, not on one who denies."
2. *Semper necessitas probandi incumbit ei qui agit* (Latin: "The necessity of proof always lies with the person who lays charges").
3. "Digital Evidence and Forensics," National Institute of Justice (NIJ), at http://www.nij.gov/topics/forensics/evidence/digital/Pages/welcome.aspx. *See also* Stephen Mason (ed.), *Electronic Evidence: Disclosure, Discovery & Admissibility,* (London: Lexis Nexis Butterworths, 2007), para. 2.03 (defining digital or e-evidence as "data comprising the output of analogue devices or data in digital format that is created, manipulated, stored or communicated by any device, computer or computer system or transmitted over a communication system, which is relevant to the process of adjudication").
4. *See supra* § 2 C.
5. *See, e.g.,* Wex, "Evidence," LII, Cornell University Law School, at https://www.law.cornell.edu/wex/evidence.
6. ITU Understanding Cybercrime, *supra* § 1 B, note 1, at 251–56.
7. Brown, *supra* § 2 C, note 8.
8. Donique Brezinski & Tom Killalea, *Guidelines for Evidence Collection and Archiving,* (RFC3227, 2002).
9. Robert O'Harrow, *No Place to Hide,* (New York: New York Free Press, (2005); Peter Stephenson, "A Comprehensive Approach to Digital Incident Investigation," Information Security Technical Report, Vol. 8, Issue 2 (2005), pp. 42–54; Aleš Završnik, "Towards an Overregulated Cyberspace," Masaryk University Journal of Law & Technology, Vol. 4, Issue 2 (2010), pp. 173–90.
10. *See infra* § 2 E, box 2.7.
11. For an overview of different kinds of evidence that can be collected by computer forensic experts, *see* Nolan *et al., supra* § 2 C, note 42.
12. Oxford English Dictionary.
13. *See* ITU Understanding Cybercrime, *supra* § 1 B, note 1; Giordano, *supra* § 2 C, note 18, at 162; Vacca, *supra* § 2 C, note 44, at 21; Ruibin & Gaertner, *supra* § 2 C, note 32; Mark Reith, Clint Carr & Gregg Gunsch, "An Examination of Digital Forensic Models," International Journal of Digital Evidence, Vol. 1, Issue 3 (2002), p. 3; Ashok Patel & Séamus Ó Ciardubhain, "The Impact of Forensic Computing on Telecommunication," IEEE Communications Magazine, Vol. 38, No. 11 (2000), p. 64, at http://ieeexplore.ieee.org/document/883490/. *See also* Mathew Hannan, "To Revisit: What Is Forensic Computing," *Australian Computer, Network & Information Forensics Conference,* (Perth, Western Australia, 25 Nov. 2004), at https://www.semanticscholar.org/paper/To-Revisit-What-is-Forensic-Computing-Hannan/7fc8d1c9d7fbdb7368685368954c24fc20139cc2 Barbara Etter, "The Forensic Challenges of E-Crime," Australasian Centre for Policing Research, No. 3 (2001), p. 4, at https://pdfs.semanticscholar.org/15c3/5e8721507feee65d5927bf9d909c9ed1497a.pdf. Regarding the need for standardization, *see* Matthew Meyers & Marc Rogers, "Computer Forensics: The Need for Standardization and Certification," International Journal of Digital Evidence, Vol. 3, Issue 2 (2004), at www.utica.edu/academic/institutes/ecii/publications/articles/A0B7F51C-D8F9-A0D0-7F387126198F12F6.pdf; Carrie Morgan Whitcomb, "An Historic Perspective of Digital Evidence: A Forensic Scientist's View," International Journal of Digital Evidence, Vol. 1, Issue 1 (2002), at https://www.utica.edu/academic/institutes/ecii/publications/articles/9C4E695B-0B78-1059-3432402909E27BB4.pdf; Gregory Hall & Wilbon Davis, "Towards Defining the Intersection of Forensic and Information Technology," International Journal of Digital Evidence, Vol. 4, Issue 1 (2005), at https://www.utica.edu/academic/institutes/ecii/publications/articles/B49F0174-F1FB-FE05-EBBB4A8C87785039.pdf; Ryan Leigland & Axel W. Krings, "A Formalization of Digital Forensics," International Journal of Digital Forensics, Vol. 3, Issue 2 (2004), at http://people.cs.ksu.edu/~sathya/formalizing-df.pdf.
14. *See* Vacca, *supra* § 2 C, note 44, at 21.
15. *See infra* § 3 B for a discussion of informal methods of international cooperation, including 24/7 networks and information sharing and coordination centers.
16. *See, e.g.,* "10 Modern Forensic Science Technologies," Forensic Colleges & Universities, at http://www.forensicscolleges.com/blog/resources/10-modern-forensic-science-technologies.
17. For an overview of different forensic investigation techniques related to the most common technologies, *see* Megan Carney & Marc Rogers, "The Trojan Made Me Do It: A First Step in Statistical Based Computer Forensics Event Reconstruction," International Journal of Digital Evidence, Vol. 2, Issue 4 (2004); Eoghan Casey, "Practical Approaches to Recovering Encrypted Digital Evidence," International Journal of Digital Evidence, Vol. 1, Issue 3 (2002), at www.utica.edu/academic/institutes/ecii/publications/articles/A04AF2FB-BD97-C28C-7F9F4349043FD3A9.pdf; Orin Kerr, "Searches and Seizures in a Digital World," Harvard Law Review, Vol. 119 (2005), p. 531 *et seq.*; Nolan *et al., supra* § 2 C, note 42; Jason Siegfried, Christine Siedsma, Bobbie-Jo Countryman & Chester D. Hosmer, "Examining the Encryption Threat," International Journal of Digital Evidence, Vol. 2, Issue 3 (2002), at www.utica.edu/academic/institutes/ecii/publications/articles/A0B0C4A4-9660-B26E-12521C098684EF12.pdf; Benjamin Turnbull, Barry Blundell, & Jill Slay, "Google Desktop as a Source of Digital Evidence," International Journal of Digital Evidence, Vol. 5, Issue 1 (2006); Matthew Kiley, Tim Shinbara & Marcus Rogers, "iPod Forensics," International Journal of Digital Evidence, Vol. 4, Issue 2 (2007); Gaurav Gupta & Chandan Mazumdar, "Digital Forensic Analysis of E-Mails: A Trusted E-Mail Protocol," International Journal of Digital Evidence, Vol. 2, Issue 4 (2007); Mayank R. Gupta, Michael D. Hoeschele & Marcus K. Rogers, "Hidden Disk Areas: HPA and DCO," International Journal of Digital Evidence, Vol. 5, Issue 1 (2006); Carole E. Chaski, "Who's at the Keyboard? Authorship Attribution in Digital Evidence Investigations," International Journal of Digital Evidence, Vol. 4, Issue 1 (2005); Ty Howard, "Don't Cache Out Your Case: Prosecuting Child Pornography Possession Laws Based on Images Located in Temporary Internet Files," Berkeley Technology Law Journal, Vol. 19 (2004), p. 1233; Dario Forte, "Analyzing the Difficulties in Backtracing Onion Router Traffic," International Journal of Digital Evidence, Vol. 1, Issue 3 (2002), at www.utica.edu/academic/institutes/ecii/publications/articles/A04AA07D-D4B8-8B5F-450484589672E1F9.pdf.

18. Warren Harrison, George Heuston, Mark Morrissey, Aucsmith & Sarah Mocas, "A Lesson Learned Repository for Computer Forensics," International Journal of Digital Evidence, Vol. 1, Issue 3 (2002).

19. Ruibin & Gaertner, *supra* § 2 C, note 32.

20. ITU Understanding Cybercrime, *supra* § 1 B, note 1.

21. Nolan *et al.*, *supra* § 2 C, note 42, at 171.

22. Regarding the challenges of encryption, *see* § 1 D; *see also* Siegfried, *supra* note 17.

23. Regarding possible counter strategies for law enforcement, *see* J. Alex Halderman, Seth D. Schoen, Nadia Heninger *et al.*, *Lest We Remember: Cold Boot Attacks on Encryption Keys,* Proc. 17th USENIX Security Symposium, (San Jose, CA, Jul. 2008), at http://citp.princeton.edu/memory.

24. Nolan *et al.*, *supra* § 2 C, note 42, at 88.

25. Vaciago, *supra* § 2 C, note 33.

26. *See Vacca, supra* § 2 C, note 44, at 43; Robert Moore, "To View or Not to View: Examining the Plain View Doctrine and Digital Evidence," American Journal of Criminal Justice, Vol. 29, No. 1 (2004), p. 59.

27. Moore, *ibid.*, at 58.

28. Lange & Nimsger, *supra* § 2 C, note 14, at 6; Gary Gordon, Chet Hosmer, Christine Siedsma & Don Rebovich, *Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime,* (Washingtong, DC: US Dept. of Justice, Jan. 2003), p. 38, at https://www.ncjrs.gov/pdffiles1/nij/grants/198421.pdf.

29. *Ibid.*

30. Consider, for instance, the issue of the FBI attempting to unlock a recovered Apple iPhone. *See supra* § 1 B, case 1.3.

31. Casey, *supra* note 17.

32. Lange & Nimsger, *supra* § 2 C, note 16, at 473; Gordon *et al.*, *supra* note 28; Marco Gercke, "Challenges Related to the Fight against Cybercrime," *Multimedia und Recht,* (2008), p. 297.

33. *See, e.g.*, Vindu Goel, "Encryption Is More Important, and Easier, Than Ever By," New York Times, (14 Oct. 2015), at http://bits.blogs.nytimes.com/2015/10/14/encryption-is-more-important-and-easier-than-ever/?_r=0.

34. Siegfried, *supra* note 17. Regarding the decryption process in forensic investigations, *see* Gordon *et al.*, *supra* note 28, at 59.

35. *Ibid.* Regarding the forensic software magic lantern, developed as a keylogger used by law enforcement in the United States, *see* Christopher Woo and Miranda So, "The Case for Magic Lantern, Highlights the Need for Increased Surveillance," Harvard Journal of Law & Technology, Vol. 15, No. 2 (2002), p. 521 *et seq.; Spyware: Background and Policy issues for Congress,* US Congressional Research Service (CRS) Report, (2007), p. 3; Thomas Green, "FBI Magic Lantern reality check," Register, (12 Mar. 2001), at www.theregister.co.uk/2001/12/03/fbi_magic_lantern_reality_check/; Alex Salkever, "A Dark Side to the FBI's Magic Lantern," Bloomberg, (27 Nov. 2001), at https://www.bloomberg.com/news/articles/2001-11-26/a-dark-side-to-the-fbis-magic-lantern; Bob Sullivan, "FBI Software Cracks Encryption Wall," NBC News, (20 Nov. 2001), at http://www.nbcnews.com/id/3341694/ns/technology_and_science-security/t/fbi-software-cracks-encryption-wall; Elinor Abreu, "FBI Confirms 'Magic Lantern' Project Exists," Rense, (13 Dec. 2001), at http://www.rense.com/general17/FBIconfirmsmagic.htm.

36. *See infra* § 3 B for discussion informal international cooperation encouraging information sharing and coordination centers.

37. Regarding the plans of German law-enforcement agencies to develop a software to remotely access a suspect's computer and perform search procedures, *see* John Blau, "Debate Rages over German Government Spyware Plan," Infoworld, (5 Sep. 2007), at http://www.infoworld.com/article/2649377/security/debate-rages-over-german-government-spyware-plan.html; Anne Broache, "Germany Wants to Sic Spyware on Terror Suspects," CNet News, (31 Aug. 2007), at https://www.cnet.com/news/germany-wants-to-sic-spyware-on-terror-suspects.

38. Erin Kenneally, "Confluence of Digital Evidence and the Law: On the Forensic Soundness of Live-Remote Digital Evidence Collection," UCLA Journal of Law & Technology, Vol. 9, No. 2 (2005).

39. *See* Vacca, *supra* § 2 C, note 42, at 52.

40. *See, e.g.*, "About Us," American Board of Criminalistics, at http://www.criminalistics.com/.

41. Kerr, *supra* note 17, at p. 538.

42. "Computer Forensics Tool Testing Project," National Institute of Standards and Technology (NIST), at http://www.cftt.nist.gov.

43. Moore, *supra* note 26, at 58.

44. *See* Casey, *supra* § 2 C, note 49, at 16; Vacca, *supra* § 2 C, note 44, at 39.

45. Chet Hosmer, "Proving the Integrity of Digital Evidence with Time," International Journal of Digital Evidence, Vol. 1, No. 1 (2001), p. 1, at www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf.

46. Whitcomb, *supra* note 13.

47. Regarding the related procedural instrument, *see* Art. 19.3, Budapest Convention, *supra* § 1 B, note 32.

48. The bit-streaming method consecutively duplicates digital data in its minimum unit–bit. This method enables replication of all data, including those hidden or deleted from the original storage device.

49. Korea: "Rule on the Collection and Analysis of Evidence by Digital Forensic Investigator," at http://www.law.go.kr/main.html *(in Korean).*

50. ITU Understanding Cybercrime, *supra* § 1 B, note 1, at 251–79.

51. *See* Nolan *et al.*, *supra* § 2 C, note 42, at 12.

52. Tom Talleur, "Digital Evidence: The Moral Challenge," International Journal of Digital Evidence, Vol. 1, Issue 1 (2002), p. 1 *et seq.*, at https://www.utica.edu/academic/institutes/ecii/publications/articles/9C4E398D-0CAD-4E8D-CD2D38F31AF079F9.pdf; Eoghan Casey, "Error, Uncertainty, and Loss in Digital Evidence," International Journal of Digital Evidence, Vol. 1, Issue 2 (2002), at www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

53. *See* UNODC Cybercrime Study, *supra* § 2 C, note 42, at 39 *et seq.*; Nolan *et al.*, *supra* § 2 C, note 42, at 85; Gordon, *supra* note 28, at 41 *et seq.*

54. Ruibin & Gaertner, *supra* note 13.

55. Gordon, *supra* note 28, at 62.

56. UNODC Cybercrime Study, *supra* § 1 C note 7, at 159, provides that "Hearsay is often defined as 'evidence given of a statement made on some other occasion, when intended as evidence of the truth of what was asserted' (Halbury's Laws, Vol. 17). Certain types of digital evidence may strictly constitute hearsay, but could be admitted under exceptions such as 'business records.'" For details, *see* Leigland & Krings, *supra* § 2 C, note 11.

57. *See, e.g., ibid.,* at 167.

58. *See, e.g.,* John H. Wigmore, "The History of the Hearsay Rule," Harvard Law Review, Vol. 17, No. 7 (1904), pp. 437–58.

59. United Kingdom: § 114(1) Criminal Justice Act 2003.

60. *Ibid.*

61. *See, e.g.,* Charles T. McCormick, et al., *McCormick on Evidence,* 4th ed., (St. Paul, MN: West Pub, 1992), p. 428.

62. Korean Criminal Procedure Act, supra § 2 C, note 14, at Art. 310 *et seq.*, ("[…] any document which contains a statement in place of the statement made at a preparatory hearing or during trial, or any statement the import of which is another person's statement made outside preparatory hearing or at the time other than the trial date, shall not be admitted as evidence.").

63. *See, e.g.,* Jeremy A. Blumenthal, "Shedding Some Light on Calls for Hearsay Reform: Civil Law Hearsay Rules in Historical and Modern Perspective," Pace International Law Review, Vol. 13, No. 1 (2001), at http://digitalcommons.pace.edu/cgi/viewcontent.cgi?article=1205&context=pilr.

64. Junsik Jang, "The Current Situation and Countermeasures to Cybercrime and Cyber-Terror in the Republic of Korea," 140th International Training Course Visiting Experts' Papers. Resource Material Series, No. 79 (2008), UNAFEI, p. 52, at http://www.unafei.or.jp/english/pdf/RS_No79/No79_08VE_Jang1.pdf (*in English*).

65. Supreme Court of Korea, Decision, 99Do2317 (3 Sep. 1999), at http://www.law.go.kr/%ED%8C%90%EB%A1%80/(99%EB%8F%842317) *(in Korean). See* Oh Gi-du, "Statement of Defendant and Authentication of Electronic Documents," Supreme Court Law Journal, Vol. 3, No. 2 (Dec. 2013), p. 73, at http://library.scourt.go.kr/SCLIB_data/publication/m_531306_v.3-2.pdf (*in English*).

66. For details, Korean Criminal Procedure Act, *supra* § 2 C, note 14, at Art. 310-2.

67. Supreme Court of Korea, *supra* note 65.

68. Korean Criminal Procedure Act, *supra* § 2 C, note 14, at Art. 316. ("(1) If a statement made by a person other than a criminal defendant […] at a preparatory hearing or a trial conveys a statement of the criminal defendant, such statement shall be admissible as evidence only if it is proved that the statement was made in a particularly reliable state. (2) Oral testimony given by a person other than the criminal defendant at a preparatory hearing or during a trial, the import of which is the statement of a person other than the criminal defendant, shall be admissible as evidence only when the person making the original statement is unable to testify because he/she is dead, ill, or resides abroad, his/her whereabouts is not known, or there is any other similar reason, and only when there exist circumstances which lend special credibility to such testimony.").

69. *Ibid.,* Pre-trial hearings are to be conducted pursuant to Art. 313(1).

70. Supreme Court of Korea, Decision 2006Do2556 (25 Nov. 2008), at http://www.law.go.kr/precInfoP.do?precSeq=125192 (*in Korean*). *See also* Blumenthal, *supra* note 63, at 72.

71. *See, e.g.,* Korea: Act on Promotion of Information and Communications Network Utilization and Information Protection, Art. 44-7, at http://elaw.klri.re.kr/kor_service/converter.do?hseq=7288&type=PDF (*in English*).

72. *See* Jang, *supra* note 64, at 72.

73. Supreme Court of Korea, Decision 99Do1252 (25 Feb. 2000), at http://www.law.go.kr/%ED%8C%90%EB%A1%80/(99%EB%8F%841252) (*in Korean*).

74. Lee Sook-yeon, "Admissibility and Examination of Digital Evidence: With a Focus on the Criminal Procedure," Supreme Court Law Journal, Vol. 2, No. 2 (2012), p. 77, at http://library.scourt.go.kr/SCLIB_data/publication/m_531306_v.2-2.pdf (*in English*).

75. As discussed further on, INTERPOL has already established information sharing and coordination centers, which might be used as places of instruction and knowledge sharing. *See* § 3 B, below.

76. UNODC already sets evidentiary standards.

Referenced in: § E. Jurisdictional Issues

1. Oxford English Dictionary.
2. Kim Soukieh, "Cybercrime–The Shifting Doctrine of Jurisdiction," Canberra Law Review, Vol. 10 (2011), pp. 221–38.
3. *See, e.g., Babcock v. Jackson,* 191 N.E.2d 279 (N.Y. 1963). The collective *corpus* of procedural law devoted to the matter determining the legal system and the law of jurisdiction applying to a given legal dispute is known as conflicts of laws at large, although (especially in civil law jurisdictions) those matters are often addressed in private and, to a lesser extent, in public international law. *See, e.g.,* Robert C. Lawrence, III, *International Tax and Estate Planning* (3d ed. 1999), Ch. 1. The ability and means of a court of the forum jurisdiction to resolve conflicts of laws is in and of itself an exertion of jurisdiction. *See ibid.* For that and other reasons, the Budapest Convention does nothing more than allow, "When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution." Budapest Convention, *supra* § 1 B, note 32, at Art. 22.5 (*emphasis added*). *See also* Budapest Explanatory Report, *supra* § 1 D, note 14, at para. 239.
4. It bears noting that while there are positive jurisdictional conflicts—where several states seek jurisdiction over the same crime—, negative ones, where no state claims jurisdiction, also exist. To limit the occurrence of the latter scenario for cybercrimes—which could potentially leave would-be plaintiffs without any recourse—, the Budapest Convention, for one, lists the bases on which a country may or must assert jurisdiction over a crime covered (Arts. 2–11), as well as obliging signatories to establish those acts as criminal offenses in their jurisdictions (Art. 22 *et seq.*). *See* Budapest Convention, *supra* § 1 B, note 32. Principles of sovereignty allows that Parties to the Convention are in no way limited in asserting jurisdiction over other crimes pursuant to their domestic law, and independent of the Convention. *See, e.g., ibid.,* at Art. 22.4.
5. *See* §§ 2 C, 2 D & 3 C.
6. *See* § 3 D.
7. Brenner, *supra* § 1 B, note 2.
8. Max Weber, "Politics as a Vocation," Max Weber: Essays in Sociology, (Oxford: Oxford University Press, 1946), pp. 77–128, at http://polisci2.ucsd.edu/foundation/documents/03Weber1918.pdf.
9. Mark Landler, "A Filipino Linked to 'Love Bug' Talks about his License to Hack," New York Times, (21 Oct. 2000), at http://www.nytimes.com/2000/10/21/business/a-filipino-linked-to-love-bug-talks-about-his-license-to-hack.html.
10. Lorenzo Franceschi-Bicchierai, "Love Bug: The Virus That Hit 50 Million People Turns 15," Motherboard, (4 May 2015), at http://motherboard.vice.com/read/love-bug-the-virus-that-hit-50-million-people-turns-15.
11. Landler, *supra* note 9.
12. The basis for international public law is by and large built upon the notion of Westphalian sovereignty. *See, e.g.,* Andreas Osiander, "Sovereignty, International Relations, and the Westphalian Myth," International Organization, Vol. 55, (2001), pp. 251–87.
13. *See, e.g.,* Budapest Convention, *supra* § 1 B, note 32, at Art. 22.1 *et seq.*,.
14. Korea: Criminal Act, (30 Dec. 2014) [hereafter, "Korean Criminal Act"], at http://www.oecd.org/site/adboecdanti-corruptioninitiative/46816472.pdf, Art. 2.
15. *See, e.g.,* Budapest Convention, *supra* § 1 B, note 32, at Art. 22.1.b.
16. *Ibid.,* at Art. 22.1.c.
17. Convention on the Law of the Sea, (10 Dec. 1982) UN Doc A/Conf.62/122, UN Reg. No I-31363, Part VII High Seas, § 1 General Provisions, Art. 87; *see also, e.g.,* Budapest Convention, *supra* § 1 B, note 32, at Art. 4., ("This Act shall apply to aliens who commit crimes on board a Korean vessel or Korean aircraft outside the territory of the Republic of Korea.").
18. *Ibid. See* Warsaw Summit Communiqué, *supra* § 1 A, note 12.
19. Budapest Convention, *supra* § 1 B, note 32.
20. ITU Understanding Cybercrime, *supra* § 1 B, note 1, at 235–38; Brenner & Koops, "Approaches to Cybercrime Jurisdiction," p. 6.
21. *See, e.g.,* 1999 Revision of the Model State Computer Crimes Code, § 1.03 (A-E), http://www.crime-research.org/library/Model.htm.
22. *See, e.g.,* Budapest Explanatory Report, *supra* § 1 D, note 4, at para. 233.
23. *Ibid.*
24. *See, e.g.,* Abraham D. Sofaer, Seymour E. Goodman, Mariano-Florentino Cuéllar *et al.,* "A Proposal for an International Convention on Cyber Crime and Terrorism," Hoover Institution, CRISP, CISAC & Stanford University (Aug. 2000), at http://cisac.fsi.stanford.edu/sites/default/files/sofaergoodman.pdf. Transnational fraud, for example, has led to decisions by national courts assuming jurisdiction on the basis of any significant connection to the conduct involved. Among these are the states where a fraud was planned, where an effort to defraud was initiated, where individuals worked at implementing the fraud, where or through which communications were made that were intrinsic to the fraud, where the victims were located, and where the fraud had material and intended effects. The widespread recognition of fraud as criminal activity leads states readily to find jurisdiction over such activity, despite the significant relationship particular frauds may have to other states. They tend to assume that punishing fraud will be supported by other affected states, rather than opposed as violating their sovereignty. At the very least, leaving aside the heightened dangers posed by cybercrime, the same rationale that supports such a broad assertion of jurisdiction over fraud supports a similar assertion of jurisdiction over cybercrime.
25. Budapest Convention, *supra* § 1 B, note 32, at Arts. 2–11.
26. *See, e.g.,* 1999 Revision of the Model State Computer Crimes Code, *supra* note 21; *see also* Budapest Convention, *supra* § 1 B, note 32, at Art. 22.1.d.
27. *See* Budapest Explanatory Report, *supra* § 1 D, note 14, at para. 236.
28. *Ibid.*
29. *See infra* for discussions of dual criminality. Also, in order to avoid a case of negative jurisdiction, where no state claims jurisdiction, the Budapest Convention allows that the principle of nationality might be used to prosecute an offender acting in a "place outside the territorial jurisdiction of any State". *See* Budapest Explanatory Report, *supra* § 1 D, note 14.
30. *Supra* ITU Understanding Cybercrime, supra § 1 B, note 1, at 237; *see also,* Korean Criminal Act, *supra* note 14, at Arts. 3 & 5.

31. *Ibid.*, ITU Understanding Cybercrime, at 237.

32. *LICRA and UEJF v. Yahoo! Inc. and Yahoo France, Tribunal de grande instance de Paris, Ordonnance de référé* (11 Aug. 2000); *see also, LICRA and UEJF vs. Yahoo! Inc. and Yahoo France, Tribunal de grande instance de Paris, Ordonnance de référé* (22 May 2000).

33. *Yahoo! Inc. v. LICRA and UEJF,* 433 F.3d 1199 (9th Cir. 2006).

34. France: Code pénal, Art. R645-1 (prohibiting the wearing or exhibiting in public uniforms, insignias, and emblems that recall those used by (i) an organization that declared illegal in application of Art. 9 of the Nuremberg Charter, or (ii) an individual who found guilty of crimes against humanity).

35. *Ibid.*

36. *Yahoo! Inc. v. UEJF and LICRA,* Order Denying Motion to Dismiss, (N.D. Cal. 2001), at http://cyber.law.harvard.edu/stjohns/Yahoo.html; *Yahoo! Inc. v. UEJF and LICRA,* Order Granting Motion for Summary Judgment, (N.D. Cal. 2001), at http://law.justia.com/cases/federal/district-courts/FSupp2/169/1181/2423974/.

37. *Yahoo! Inc. v. LICRA and UEJF, supra* note 33.

38. *See* Italy: *Codice penale,* Art. 7; France: Code pénal, Art. 113-10; Germany: *Strafgesetzbuch,* § 6; and Spain: *Código penal,* Art. 5, No. 1, which specifically deals, *inter alia,* with computer crime. *See also, United States v. Zehe,* 601 F. Supp. 196 (D. Mass. 1985) (where, under the Espionage Act (USC Title 18, §§ 792–99), the government brought criminal charges against an East German citizen for alleged acts of espionage—a threat to national security—against the United States committed in Mexico and in Germany); *see also,* Korean Criminal Act, *supra* note 14, at Art. 6.

39. *See, e.g.,* Damien Geradin, Marc Reysen & David Henry, "Extraterritoriality, Comity and Cooperation in EC Competition Law," SSRN, (Jul. 2008), at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1175003.

40. *See, e.g.,* J. P. Griffin, "Extraterritoriality in US and EU Antitrust Enforcement," Antitrust Law Journal, Vol. 67 (1999), p. 159. For a class case, *see United States v. Aluminum Company of America (Alcoa),* 148 F.2d 416 (2d Cir. 1945).

41. *See, e.g.,* USC Title 18,§§ 792–99 (the "Espionage Act").

42. Budapest Explanatory Report, *supra* § 1 D, note 14, at para. 237.

43. Armando Cottim, "Cybercrime, Cyberterrorism and Jurisdiction: An Analysis of Article 22 of the COE Convention on Cybercrime," European Journal of Legal Studies, Vol. 2, Issue 3 (2010), at http://www.ejls.eu/6/78UK.htm#_ftnref34.

44. *See, e.g.,* France: *Code de procédure pénal,* Art. 689 (authorizing French courts to exert jurisdiction for committing of any of the following acts beyond the French territory: torture, terrorism, nuclear smuggling, naval piracy, and airplane hijacking); *see also,* Xavier Philippe, "The Principles of Universal Jurisdiction and Complementarity: How Do the Two Principles Intermesh?," International Review of the Red Cross, Vol.88, No. 862 (2006), at https://www.icrc.org/eng/assets/files/other/irrc_862_philippe.pdf.

45. Philippe, *ibid.*

46. *See supra* § 2 A.

47. Budapest Explanatory Report, *supra* § 1 D, note 14, at para. 237–38.

48. Budapest Convention, *supra* § 1 B, note 32, at Art. 22. The Budapest Convention allows that each signatory might alter its bases for setting jurisdiction, and that those provided in the Convention are not exclusive. Budapest Explanatory Report, *supra* § 1 D, note 14, at para. 238.

49. Australia: Australian Criminal Code Act, Art.14 & 15, at http://www.austlii.edu.au/au/legis/cth/consol_act/cca1995115/sch1.html.

50. *Ibid.,* at Art. 14(1).

51. *Ibid.,* at Art.15 (14); *see also ibid.,* at Art. 16 *et seq.*

52. *Ibid.,* at Art. 14.1.

53. Gregor Urbas, "Cybercrime, Jurisdiction and Extradition," Journal of Internet Law, (2012), pp. 9–10.

54. "About the Computer Crime & Intellectual Property Section," US Dept. of Justice, at https://www.justice.gov/criminal-ccips.

55. *Ibid.*

56. *See* Karen DeYoung, "Intense Diplomacy between Secretary of State Kerry and His Iranian Counterpart to Secure Sailors," Washington Post, (13 Jan. 2016), at https://www.washingtonpost.com/news/checkpoint/wp/2016/01/13/intense-diplomacy-between-secretary-of-state-kerry-and-his-iranian-counterpart-to-secure-sailors-release/.

57. Jamie Crawford, "Kerry Tells Iran in Long Day of Calls: This Can be 'a Good Story for Both of Us', " CNN, (13 Jan. 2016), at http://www.cnn.com/2016/01/13/politics/john-kerry-iran-zarif-sailors/.

58. Budapest Convention, *supra* § 1 B, note 32, at Art. 22.5.

59. "Dual criminality" (also known as "double criminality") refers to a requirement that the act subject to a request for extradition or mutual legal assistance must be a criminal offence under the laws of both custodial and requesting States. *See, supra* § 2 A.

60. For a detailed discussion of other jurisdictional possibilities, *see* Budapest Explanatory Report, *supra* § 1 D, note 14, at para. 234–35.

Referenced in: § F. Institutional Framework

1. *See supra* § 2 C.
2. *See, e.g.,* "National Cyber Security Strategies in the World," European Union Agency for Network and Information Security (ENISA), at https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world.
3. Stuxnet virus was the name of sophisticated malicious code, believed to have been developed by US and Israeli governments, that was used to force the failure of nuclear centrifuges of the Natanz uranium enrichment plant in Iran. Rather than hijack computers themselves or steal information stored thereon, Stuxnet targeted the equipment and infrastructure controlled by those computers. Understood as the "world's first digital weapon," the air-gap—a network security measure used to ensure that a secure computer network is physically isolated from unsecured ones—was overcome, and Stuxnet introduced into the physically-isolated Natanz plant, through contaminated USB keys. It is believed to have been used as a model for the failed cyberattack on North Korean. *See, e.g.,* Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon,* (New York: Crown Publishers, 2014). Kim Zetter, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon," Wired, (3 Nov. 2014), at https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/. *See also,* Rachael King, "Stuxnet Infected Chevron's IT Network," Wall Street Journal, (8 Nov. 2012), at http://blogs.wsj.com/cio/2012/11/08/stuxnet-infected-chevrons-it-network/.
4. Joseph Menn, "Exclusive: US Tried Stuxnet-Style Campaign Against North Korea but Failed—Sources," Reuters, (29 May 2015), at http://www.reuters.com/article/us-usa-northkorea-stuxnet-idUSKBN0OE2DM20150529.
5. *See, e.g.,* "National Strategies," ITU, at www.itu.en/ITU-D/Cybersecurity/Pages/National-Strategies.aspx.
6. UK Cabinet Office and UK National Security Secretariat, "The UK Cyber Security Strategy – Protecting and Promoting the UK in a Digital World," (London: Crown, 2011), at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf.
7. *See* UK Cabinet Office and UK National Security Secretariat, "Cyber Security Strategy: Progress So Far," (London: Crown, 2013), at https://www.gov.uk/government/collections/cyber-security-strategy-progress-so-far--2.
8. *See* The Rt Hon Matt Hancock MP, UK Cabinet Office & UK National Security Secretariat, "UK Cyber Security Strategy: Statement on the Final Annual Report," (14 Apr. 2016), at https://www.gov.uk/government/speeches/uk-cyber-security-strategy-statement-on-the-final-annual-report.
9. ITU Understanding Cybercrime, *supra* § 1 B, note 1.
10. The UK Home Office is the government department responsible for immigration, counter-terrorism, police, drugs policy and related science and research. *See* "Home Office," Gov.uk, at https://www.gov.uk/government/organisations/home-office.
11. "Department for Business, Energy and Industrial Strategy (BEIS)," Gov.uk, at https://www.gov.uk/government/organisations/department-for-business-innovation-skills. The UK Cyber Security Strategy speaks of the Department for Business, Innovation and Skills (BIS); however, that office and the Department of Energy and Climate Change (DECC) have since merged to form the Department for Business, Energy and Industrial Strategy (BEIS). *Ibid.*
12. "Department for Culture, Media and Sport," Gov.uk, at https://www.gov.uk/government/organisations/department-for-culture-media-sport.
13. "Cabinet Office," Gov.uk, at https://www.gov.uk/government/organisations/cabinet-office.
14. "Ministry of Defence," Gov.uk, at https://www.gov.uk/government/organisations/ministry-of-defence.
15. "Foreign and Commonwealth Office," Gov.uk, at https://www.gov.uk/government/organisations/foreign-commonwealth-office.
16. UK National Security Secretariat, *supra* note 6.
17. *See* UK Cabinet Office & UK National Security Secretariat, "The UK Cyber Security Strategy 2011-2016: Annual Report," (14 Apr. 2016), at https://www.gov.uk/government/publications/the-uk-cyber-security-strategy-2011-2016-annual-report.
18. UK Cabinet Office, *supra* note 7.
19. Korea: Act on Promotion of Information and Communications Network Utilization and Data Protection, etc., Act 1, at http://www.worldlii.org/int/other/PrivLRes/2005/2.html *(in English).*
20. *See* "United States Secret Service Electronic Crimes Task Forces," at https://www.dhs.gov/sites/default/files/publications/USSS%20Electronic%20Crimes%20Task%20Force.pdf.
21. Michael Kraft & Edward Marks, *US Government Counterterrorism: A Guide to Who Does What,* (Boca Raton, FL: CRC Press, 2012).
22. *See* "Electronic Crimes Task Forces (ECTF)," The White House of President Barack Obama, at https://obamawhitehouse.archives.gov/files/documents/cyber/United%20States%20Secret%20Service%20-%20Electronic%20Crimes%20Task%20Forces.pdf
23. USA PATRIOT Act, *supra* § 1 C, note 10, at § 105.
24. *See* "Combatting Cyber Crime," US Dept. of Homeland Security, at https://www.dhs.gov/topic/combating-cyber-crime.
25. Sophia Yan & K.J. Kwon, "Massive Data Theft Hits 40% of South Koreans," CNNTech, (21 Jan. 2014), at http://money.cnn.com/2014/01/21/technology/korea-data-hack/.
26. *See supra* § 2 B, box 2.3.
27. Yan § Kwon, *supra* note 25.

CHAPTER 3

National Legal Frameworks

Building on the procedural, evidentiary, jurisdictional and institutional issues discussed in chapter 2, this chapter provides an overview of substantive criminal aspects of cybercrime and how they are expressed in national legal frameworks.

In this Chapter

A. Substantive Law

Table of Contents

Introduction

In chapter 2, above, the various aspects of cybercrime are addressed at a high level—first, laying out a working definition of cybercrime (*see* section 2 A), then having discussed what conduct is criminalized (*see* section 2 B), and going on to consider procedural (*see* section 2 C), evidentiary (*see* section 2 D), jurisdictional (*see* section 2 E) and institutional (*see* section 2 F) issues. This chapter tries to give a more concrete understanding of those matters. This subsection shows how the already-discussed offences appear in national laws. It also introduces the idea of the how certain safeguards—general due process issues as well as data protection and freedom of expression - appear in national law. Just as there is no one, globally accepted definition of cybercrime (*see* section 2 A, above), similarly, acts constituting cybercrime differ from state to state, with each state determining the various constitutive elements through

its own domestic processes. As a result of this fragmentation, certain behavior that is understood as criminal in one country may not necessarily be classified as criminal in another; accordingly, perpetrators may not necessarily be subject to criminal punishment largely due to the absence of dual criminality (*see* section 2 A, above).[1] In instances where criminal sanctions may not be available, civil or administrative measures may exist for specific types of individual cybercrime acts.[2]

I. Existing National Cybercriminal Legislation

While various cybercrimes have been discussed in section 2 B, above, this section, following the same construction, considers how national laws have addressed such concerns by looking at the following cybercrimes: **(A)** the unauthorized access to a computer system, or hacking, **(B)** illegal acquisition of computer data, **(C)** illegal interception of computer, **(D)** illegal access to, and interfering with, computer data, **(E)** illegal system interference, **(F)** misuse of devices, **(G)** fraud, **(H)** forgery, **(I)** spamming, **(J)** child pornography and **(K)** copyright and trademark offenses.

A. Illegal Access

Illegal access to a computer system, is, in many ways, one of the most basic cybercrimes as it enables subsequent (cyber)criminal behavior (*see* section 2 B, above). Correspondingly, that behavior is now widely, though not universally, criminalized. Many countries criminalize hacking through cyber-specific legislation,[3] while others criminalize such acts by way of a general offence.[4]

Depending on the jurisdiction's chosen approach, the perpetrator must have a certain "guilty" mental state, or *mens rea,* in order to be found culpable of this offense.[5] Some states take an approach that expands this offense beyond unauthorized access to include continued or remained access to the computer system beyond that initial unauthorized trespass, or, if authorization existed, then presence beyond the period or purposes for which that authorization was granted. Other jurisdictions classify "illegal access"—what is often termed as "unauthorized monitoring"[6]—as a separate offense under separate provisions. Some national laws make illegal access a criminal offense only if it is paired with interference to or with that data—for instance, the copying, blocking, destroying, modifying or deleting of the data[7]; others criminalize the activity only if such illegal access is committed in connection with one of the components of illegal data or system interference. It is considered good practice to avoid adding further elements to the base-level crime, as doing so might lead to difficulties in distinguishing between other offences (*e.g.,* data espionage, illegal data or system interference), as well as limiting interoperability.[8]

Box 3.1: Saint Vincent and the Grenadines
Example of Legislation Criminalizing Hacking

"A person who intentionally, without lawful excuse or justification, accesses the whole or any part of an information system commits an offence and is liable on conviction [….]"[9]

B. Illegal Acquisition of Computer Data

The illegal acquisition of computer data refers to obtaining computer data intentionally without authorization. The offense generally lies in the intentional unauthorized possession of such data alone; it does not depend on what may have been done with either that data or to the original data. However, the statutes in some countries require additional elements, such as that a person has breached security measures, or has a specific dishonest intent.

Box 3.2: Kazakhstan
Example of Legislation Criminalizing Illegal Access to Computer Data

"*Illegal access to computer information* which is protected by law, that is information on a storage medium, in a computer, computer system, or computer network, and equally violation of the rules for operation of a computer, computer system or their network by persons, [by persons and through the creation of programs for computers] who have access to the computer, computer system or their network, *if this action entailed destruction, blocking, modification, or the copying of information, or disruption of the work* of a given computer, computer system, or computer network [….]"[10]

In Germany, a wider net is cast, with any data, regardless of its status or of the acquirer's purpose, being protected from unauthorized acquisition.[11]

Box 3.3: Germany
Example of Legislation Criminalizing Illegal Access to Computer Data

"Whosoever unlawfully obtains data for himself or another that were not intended for him and were especially protected against unauthorized access, if he has circumvented the protection, shall be liable [….]"[12]

"[…] above data shall only be those stored or transmitted electronically or magnetically or otherwise in a manner not immediately perceivable."[13]

C. Illegal Interception of Computer Data

Illegal interception of computer data refers to acts involving intercepting data during transmission without authorization. At the national level, while many states cover illegal interception of computer data transmitted by cyber-specific legislation, others apply existing laws that criminalize unlawful interception of communications.[14] Further, while, in some states, the scope of the offence is unrestricted, in others it is limited to private transmissions.[15]

Box 3.4: Botswana
Example of Legislation Criminalizing Illegal Interception of Computer Data

"A person who intentionally and by technical means, without lawful excuse or justification, intercepts— (a) any non-public transmission to, from or within a computer or computer system; or (b) electromagnetic emissions that are carrying data, from a computer or computer system, commits an offence [….]"[16]

D. Illegal Interference with Computer Data

Quite similar to illegal access to computer data, illegal data interference refers to the unauthorized or unjustified interference with computer data (*e.g.*, inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing).[17]

Box 3.5: Portugal
Example of Legislation Criminalizing Illegal Data Interference

"Whoever, without legal permission or authorization from the owner or holder of the right over the full system, or part thereof, deletes, alters, fully or partially deteriorates, damages, suppresses or renders unusable or inaccessible other people's programmes or other computer data or by any other means seriously hinders their functioning, shall be punishable[….]"[18]

E. Illegal System Interference

Another variant of illegal interference, this offense criminalizes interference that substantially hinders the functioning of a computer system without authorization or justification.[19] Some states have special statutory provisions governing illegal interference with computer systems of critical national infrastructure.[20] According to UNODC, seventy percent of the countries reported the existence of a variant of this cyber-specific offence.[21] An additional twenty-two percent indicated that this act was criminalized by way of a general offence.[22]

Box 3.6: The Gambia
Example of Legislation Criminalizing Illegal System Interference

"A person who, without lawful authority or lawful excuse, does an act which causes directly or indirectly

A. A degradation, failure, interruption or obstruction of the operation of a computer system

B. A denial of access to, or impairment of any program or data stored in, the computer system, commits an offence."[23]

F. Misuse of Devices

Criminalization of the misuse of tools existed well before the development of ICTs. Misuse of devices refers to acts involving computer tools to commit cybercrimes. In the cybercriminal context, the term "tools" is broadly understood, possibly covering not only software or devices, but also passwords or codes that enable access to computer systems and data (also called "access codes").[24]

In response to growing underground markets for trading information, software and other tools used to commit crimes in cyberspace, many national laws have adopted provisions specifically targeting acts concerning computer misuse tools.[25] UNODC found that approximately sixty-seven percent of responding had cyber-specific offences concerning the misuse of computer tools.[26] About ten percent of responding countries indicated that such acts act were criminalized by way of a general offence.[27] Domestic laws typically require both that the tool be either designed or adapted for the purpose of the committing the prescribed offence, and that the perpetrator have the requisite intent.[28] Other laws, by contrast, are more expansive, either requiring only that the tool's purpose be the furtherance of a cybercriminal,[29] *or* that perpetrator presents the requisite *mens rea*.[30]

The production, distribution, making available or possession of "computer misuse tools" may also be criminalized.[31] Relatedly, the unauthorized disclosure of passwords or access codes is often also criminalized.[32]

Box 3.7: Ghana
Example of Legislation Criminalizing Misuse of Devices[33]

"A person who intentionally, recklessly, without lawful excuse or justification, possesses, produces, sells, procures for use, imports, exports, distributes or otherwise makes available

A. A device, including a computer programme, that is designed or adapted for the purpose of committing an offence

B. A computer password, access code or similar electronic record by which the whole or any part of a computer system is capable of being accessed with the intent that it be used by a person for an offence commits an offence and is liable [….]"

G. Fraud

Fraud is generally understood as consisting of some deceitful practice or willful device intentionally used to deprive another of his or her right, or to cause him or her some other harm.[34] For instance, the World Bank, which, working in an administrative system, understands the term more broadly than most, describes "fraudulent practice" as "any act or omission, including misrepresentation, that knowingly or recklessly misleads, or attempts to mislead, a party to obtain financial or other benefit or to avoid an obligation".[35] As traditional notions of fraud require the direct deception of a physical person, transitioning to cyberspace can cause legal complication since ICT-related fraud typically involves acts of data or system manipulation or interference. In order to address potential legal issues, many countries have introduced cyber-specific provisions.[36] Relatedly, while some countries incorporate unauthorized use of electronic payment tools into provisions on fraud, others criminalize such acts under stand-alone offences.[37]

Box 3.8: Korea
Example of Legislation Criminalizing ICT-related Fraud[38]

"Any person who acquires any benefits to property or has a third person acquire them, by making any data processed after inputting a false information or improper order, or inputting or altering the data without any authority into the data processor, such as computer, etc., shall be punished […]"

H. Forgery

The crime of forgery is typically understood as the false-making, with intent to defraud, of a writing (through construction, alteration or false signature), which, if genuine, would be of legal efficacy or the foundation of a legal liability.[39] ICT-related forgery is an act involving interference with computer data resulting in inauthentic data with specific intent to cause such data to be relied upon as if it were authentic.[40] According to UNODC, some countries reported having criminalizing computer-related fraud or forgery through a general offense[41]; others indicate that this act was criminalized by way of a cyber-specific offence.[42]

Similar to traditional fraud offences, forgery offences often require modification of a writing or other visual representation. That requirement often presents legal difficulties in covering ICT-related forgery which involve manipulation or alteration of computer data. To address such difficulties, some countries extend the legal definition of "document"or "writing" to include data stored on a computer system,[43] while other systems have introduced provisions explicitly addressing computer-related forgery.[44] Some countries enumerate different punishments depending on whether public or private data are subject to forgery.[45]

Box 3.9: Samoa
Example of Legislation Criminalizing ICT-related Forgery[46]

"A person is liable to […] who intentionally and without authorisation, inputs, alters, deletes, or suppresses electronic data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless of whether or not the data is directly readable and intelligible."

I. Spamming

Spamming—that is, using the internet to indiscriminately send unsolicited messages (typically to a large numbers of recipients)—is a phenomenon unique to cyberspace because of the free exchange of information and messages. According to UNODC, twenty-one percent of countries have criminalized the sending of spam.[47] A further fourteen percent of the responding countries indicated that this act was criminalized by way of a general offence.[48] Anti-spam laws typically criminalize the transmission of unsolicited, multiple electronic messages and the manipulation of either the message header or of the originating information.[49] In some countries, the unauthorized access to a protected computer and initiation of the transmission of multiple commercial electronic mail messages is also criminalized.[50]

Box 3.10: United States of America
Example of Legislation Criminalizing Sending Spam[51]

"(a) In general. —Whoever, in or affecting interstate or foreign commerce, knowingly—

(1) Accesses a protected computer without authorization, and intentionally initiates the transmission of multiple commercial electronic mail messages from or through such computer

(2) Uses a protected computer to relay or retransmit multiple commercial electronic mail messages, with the intent to deceive or mislead recipients, or any Internet access service, as to the origin of such messages

(3) Materially falsifies header information in multiple commercial electronic mail messages and intentionally initiates the transmission of such messages

(4) Registers, using information that materially falsifies the identity of the actual registrant, for five or more electronic mail accounts or online user accounts or two or more domain names, and intentionally initiates the transmission of multiple commercial electronic mail messages from any combination of such accounts or domain names

(5) Falsely represents oneself to be the registrant or the legitimate successor in interest to the registrant of 5 or more Internet Protocol addresses, and intentionally initiates the transmission of multiple commercial electronic mail messages from such addresses

or conspires to do so, shall be punished as provided in subsection (b)."

J. Child Pornography Offences

ICT-related child pornography offences criminalize the use of ICT to produce, distribute, access, store or possess child pornography. According to UNODC, sixty-five percent of responding countries reported generally criminalizing child pornography—for instance, by including language such as "by any means" or "in any manner".[52] A further fourteen countries indicated that the offence was criminalized by way of a cyber-specific instrument or element—for instance, by having language such as "through computer systems".[53] Other countries have criminalized ICT-related child pornography through judicial interpretation of general obscenity laws, or by extending a legal definition of "child pornography" to cover child pornographic material in the form of computer data.[54]

Box 3.11: Estonia
Example of Legislation Criminalizing ICT-related Child Pornography Offence[55]

"A person who manufactures, stores, hands over, displays or makes available in any other manner pictures, writings or other works or reproductions of works depicting a person of less than 18 years of age in a pornographic situation, or a person of less than 18 years of age in a pornographic or erotic situation shall be punished [….]"

K. Copyright & Trademark Offences

Copyright and trademark laws protect a party's branding and good name from unauthorized usage—trademarks, by identifying and distinguishing the source of the goods, and copyrights, by protecting original works of authorship. Analogs in cyberspace do much the same thing, focusing on limiting those who can claim to have authored or created a work, as well as who can posture as producing products.[56] Roughly seventy-one percent of countries responding to UNODC's survey reported having criminalized computer-related copyright and trademark offence.[57] An additional 14 percent indicated that cyber-specific provisions were in place.[58]

Box 3.12: United States of America
Example of Legislation Criminalizing ICT-related Copyright Offence[59]

"(1) In general. —Any person who willfully infringes a copyright shall be punished as provided under section 2319 of title 18, if the infringement was committed—

(A) For purposes of commercial advantage or private financial gain

(B) By the reproduction or distribution, including by electronic means, during any 180-day period, of 1 or more copies or phonorecords of 1 or more copyrighted works, which have a total retail value of more than $1,000

(C) By the distribution of a work being prepared for commercial distribution, by making it available on a computer network accessible to members of the public, if such person knew or should have known that the work was intended for commercial distribution."

II. Safeguards

The other key area to be reflected in national legislation are the safeguards accompanying the criminal sanctions. Although these are discussed more at length in greater depth in the sections 4 A and 4 B, below, it bears highlighting here that ensuring that fundamental rights are protected is as important as criminalizing certain behaviors. Fundamental freedom requiring protection include **(A)** due process, **(B)** privacy and data and **(C)** freedom of expression.

A. General Due Process Considerations

A number of procedural issues related to investigations and prosecutions are considered in section 2 C; other issues related to due process, such as the rights of the accused to counsel and to being present in connection with certain digital investigations. A vast area for consideration, the Toolkit does not exhaustively deal with the full range of due process issues related generally to criminal law; rather it focuses on specific issues related to cybercrime.

B. Privacy & Data Protection

According to UNODC, almost all responding countries indicated that existing privacy protections extended to computer data and electronic communications.[60] A balance is struck by protecting the privacy of personal data collected and processed by third parties, while allowing, in exceptional circumstances, that these third parties could be obliged to make disclosures to law enforcement.[61]

C. Freedom of Expression

Freedom of expression must be taken into account in criminalizing the dissemination of information via computer systems or cyberspace either because the underlying content is illegal (*e.g.*, child pornography, or because the actor is unauthorized to do so (*e.g.*, copyright).[62] Relatedly, the responsibility of facilitators (*e.g.*, ISPs) must be taken into account, with many countries limiting liability.[63]

Conclusion

There is a diversity of ways in which states have defined, criminalized and instituted procedural, evidentiary, jurisdictional and institutional aspects in fight against cybercrime. This section has highlighted just a few of the very many options by which national substantive law has criminalized various cybercrimes, with selection being based on good practices and with an eye to furthering international interoperability. In addition to appropriately empowering authorities to combat cybercrime, it is important to ensure that corresponding safeguards—notably for due process, privacy and data and freedom of expression—are also implemented.

End Notes

Referenced in: § A. Substantive Law

1. *See supra* § 2 E, box 2.7 (discussing the inability of domestic law enforcement to prosecute the creator of the "love bug" virus, and of foreign law enforcement authorities to arrange for extradition, due to the absence of domestic law criminalizing computer hacking).
2. UNODC Cybercrime Study, *supra* § 1 C, note 7, at 78.
3. UNODC, "Cybercrime Questionnaire for Member States", (2012) [hereafter, "UNODC Questionnaire"], Q25, at https://cms.unov.org/DocumentRepositoryIndexer/GetDocInOriginalFormat.drsx?DocID=f4b2f468-ce8b-41e9-935f-96b1f14f7bbc.
4. UNODC Cybercrime Study, *supra* § 1 C, note 7, at 82.
5. The principle is captured by the Latin dictum "*actus reus non facit reum nisi mens sit rea*" ("the act is not culpable unless the mind is guilty"). *See, e.g.,* Oxford Reference. For an overview of the different legal approaches to criminalize illegal access to computer systems, *see* Stein Schjolberg, *The Legal Framework – Unauthorized Access to Computer Systems: Penal Legislation in 44 Countries* (Moss District Court, Norway, 2003), at http://www.mosstingrett.no/info/legal.html#24.
6. *See supra* § 2 B.
7. *See, e.g.,* Kazakhstan: Criminal Code, No. 167 (16 Jul. 1997), Art. 227.1, at http://www.parliament.am/library/Qreakan/kazakstan.pdf.
8. *Supra* note 2, at 83–84.
9. Saint Vincent and the Grenadines: Electronic Transactions Act, (2007), § 66, at http://www.oas.org/juridico/spanish/cyb_svg_electronic_act_2007.pdf.
10. *See, e.g.,* Kazakhstan Criminal Code, *supra* note 7 at Arts. 227.1–227.4 (applying to persons (Art. 227.1), to groups of person (Art. 227.2) and to computer programs (Art. 227.3)) (*emphasis added*).
11. *See, e.g.,* Germany: Criminal Code, § 202a, at http://www.gesetze-im-internet.de/englisch_stgb/german_criminal_code.pdf.
12. *Ibid.,* at § 202a(1).
13. *Ibid.,* at § 202a(2).
14. *See, e.g.,* Korea: Protection of Communications Secrets Act, No. 6626 (2002),Arts. 3 & 16(1)(1), at https://www.imolin.org/doc/amlid/Republic_of_Korea_Protection_of_Communications_Secrets_Act.pdf. *See also,* UNODC Cybercrime Study, *supra* § 1 C, note 7, at 86.
15. UNODC Cybercrime Study, *supra* § 1 C, note 7, at 87.
16. Botswana: Cybercrime Act, No. 22 (2007), Ch. 08:06: Cybercrime and Computer Related Crimes, § 9, at https://hingx.org/Share/Details/711.
17. UNODC Cybercrime Study, *supra* § 1 C, note 7, at 89–90.
18. Portugal: Cybercrime Law, No. 109 (15 Sep. 2009), Art. 4.1, at http://www.wipo.int/edocs/lexdocs/laws/en/pt/pt089en.pdf.
19. UNODC Cybercrime Study, *supra* § 1 C, note 7, at 90–91.
20. *See, e.g.,* Korea: Act on the Protection of Information and Communications Infrastructure, No. 11690 (23 Mar. 2013), Art. 12 (Prohibition against Intrusion, etc. of Critical Information and Communications Infrastructure) and Art. 28 (Penal Provisions), at http://elaw.klri.re.kr/eng_mobile/viewer.do?hseq=28812&type=part&key=43.
21. UNODC Questionnaire, *supra* note 3, at Q27.
22. UNODC Cybercrime Study, *supra* § 1 C, note 7, at 88 (Figure 4.9: Criminalization of illegal data interference or system damage).
23. Gambia: Information and Communications Act, (2009), [hereafter, "Gambian Act"] § 167(1), at http://www.wipo.int/edocs/lexdocs/laws/en/gm/gm006en.pdf.
24. UNODC Cybercrime Study, *supra* § 1 C, note 7, at 93.
25. *Ibid.,* at 92–93.
26. UNODC Questionnaire, *supra* note 3, at Q28.
27. UNODC Cybercrime Study, *supra* § 1 C, note 7, at 93 (Figure 4.16: Criminalization of production, distribution, or possession of computer misuse tools).
28. *See, e.g.,* Ghana: Electronic Transactions Act, No. 772 (2008) [hereafter, "Ghanian Act"], § 135 (Illegal devices), at http://www.researchictafrica.net/countries/ghana/Electronic_Transactions_Act_no_772:2008.pdf.
29. Gambian Act, *supra* note 23, at § 10 (Unlawful possession of devices or data).
30. *See, e.g.,* Sri Lanka: Computer Crimes Act, No. 24 (2007), § 9, at http://www.slcert.gov.lk/Downloads/Acts/Computer_Crimes_Act_No_24_of_2007(E).pdf; UNODC Cybercrime Study, *supra* § 1 C, note 7, at 94.
31. UNODC Cybercrime Study, *supra* § 1 C, note 7, at 95.
32. *See, e.g.,* Antigua and Barbuda: Electronic Crimes Act, No. 14 (2013) § 9, at http://laws.gov.ag/acts/2013/a2013-14.pdf.
33. Ghanaian Act, *supra* note 28, at § 135.
34. Black's Law Dictionary.
35. *See, e.g.,* "What is Fraud and Corruption?," Integrity Vice Presidency, World Bank, at http://www.worldbank.org/en/about/unit/integrity-vice-presidency/what-is-fraud-and-corruption.
36. *See, e.g.,* Korean Criminal Act, *supra* § 2 E, note at 14, at Art. 347-2; UNODC Cybercrime Study, *supra* § 1 C, note 7, at 98–99.
37. *See, generally, supra* § 2 B.
38. Korean Criminal Act, *supra* § 2 E, note 14, at Art. 347-2.
39. Black's Law Dictionary.
40. UNODC Cybercrime Study, *supra* § 1 C, note 7, at 98–99.
41. UNODC Questionnaire, *supra* note 3, at Q 30.
42. UNODC Cybercrime Study, *supra* § 1 C, note 7, at 97 (Figure 4.21: Criminalization of computer-related fraud or forgery).

43. *See, e.g.,* Zimbabwe: Criminal Law (Codification and Reform) Act (No. 23 of 2004), § 135 (Interpretation in Part IV of Chapter VI) and § 137(1) (Forgery), at https://www.unodc.org/tldb/pdf/Zimbabwe/ZIM_Crim_Law_2004.pdf.

44. *See, e.g.,* Korean Criminal Act, *supra* § 2 E, note 14, at Art. 227-2 (False Preparation or Alteration of Public Electromagnetic Records) and Art. 232-2 (Falsification or Alteration of Private Electromagnetic Records).

45. *Ibid.*

46. Samoa: Crimes Act, No. 10 (2013), § 216, at https://www.unodc.or.g/res/cld/document/wsm/2013/crimes_act_2013_html/Samoa_Crimes_Act_2013.pdf.

47. UNODC Questionnaire, *supra* note 3, at Q 33.

48. UNODC Cybercrime Study, *supra* § 1 C, note 7, at 95 (Figure 4.20: Criminalization of the sending or controlling of the sending of SPAM).

49. *Ibid.*, at 96.

50. *See, e.g.,* United States: USC, Title 18, § 1037. *See also,* ITU Understanding Cybercrime, *supra* § 1 B, note 1, at 208.

51. USC, Title 18, § 1037.

52. UNODC Questionnaire, *supra* note 3, at Q36.

53. UNODC Cybercrime Study, *supra* § 1 C, note 7, at 101 (Figure 4.23: Criminalization of computer-related production, distribution or possession of child pornography").

54. For details, *see ibid.*

55. Estonia: Penal Code, (6 Jun. 2001), § 178(1), at https://www.unodc.org/res/cld/document/estonia-criminal-code-as-amended-2013_html/Estonia_Criminal_Code_as_amended_2013.pdf.

56. *See, e.g.,* United States: USC Title 17, § 506 (Criminal offenses), at https://www.gpo.gov/fdsys/pkg/USCODE-2010-title17/pdf/USCODE-2010-title17-chap5-sec506.pdf.

57. UNODC Questionnaire, *supra* note 3, at Q32.

58. UNODC Cybercrime Study, *supra* § 1 C, note 7, at 105 (Figure 4.29: Criminalization of computer-related copyright and trademark offences).

59. UNODC Questionnaire, *supra* note 3, at Q32.

60. *Ibid.*, at Q21.

61. *See, e.g.,* Korea: Personal Information Protection Act, No. 11990 (6 Aug. 2013) Arts. 3(6) & 18(2)(7), at http://elaw.klri.re.kr/eng_mobile/viewer.do?hseq=28981&type=part&key=4. *See also,* UNODC Cybercrime Study, *supra* § 1 C, note 7, at 135–36.

62. *See, e.g.,* Schjolberg, *supra* note 5, at 21.

63. *See, e.g.,* Korea: Copyright Law, No. 9625 (22 Apr. 2009), Arts. 102 & 104(1), at http://www.copyright.or.kr/eng/laws-and-treaties/copyright-law/chapter06.do. *See* UNODC Cybercrime Study, *supra* § 1 C, note 7, at 253.

Safeguards

While issues of procedural due process, protection of data and privacy and freedom of expression could be included in a discussion of national legal frameworks, they are treated separately in this chapter because of the importance of such legal "safeguards". This chapter examines procedural due process, data protection/privacy and freedom of expression as they relate to cybercrime.

In this Chapter

A. Due Process

Table of Contents

Introduction

As stated in the WDR,[1] for an ICT ecosystem to be vibrant and to contribute to economic development, it needs to be built around a "trust" environment. Part of that trust environment is ensuring the security of networks, systems and data; but the trust environment is equally built around preserving the individual's privacy and protecting data about those individuals, as well as ensuring rights of online expression. Efforts at combatting cybercrime tend to aim at the security part; however, as part of the overall trust environment, a cybercrime regime must also pay due regard to preserving individual rights in a balanced way.

This section considers due process issues generally, and then focuses on data protection and freedom of expression in subsequent sections. A comprehensive overview of due process rights in investigating and prosecuting crimes is beyond the scope of this Toolkit *writ large*, and this section in particular. The Toolkit generally operates and is constructed from the perspective that whatever due process rights exist in the case of "conventional" crimes would also apply to cybercrimes. This section attempts to put due process rights of general application in the specific cybercrime context by looking at how such rights were handled in recent high-profile cases, as well as how one country, Korea, has attempted to grapple with these issues.

I. Concept of Due Process

The concept of due process of law and respect for the rule of law is recognized as fundamental to both common and civil law systems.[2] Many constitutions offer explicit due process guarantees. For example, the Fifth and the Fourteenth Amendments to the US Constitution provide that "No person shall be […] deprived of life, liberty or property, without due process of law." Likewise, Korea, which has a more civil law-oriented legal system, has similar clauses in its Constitution. Specifically, Article 12 of the Korean Constitution provides that,"All citizens shall enjoy personal liberty. No person shall be arrested, detained, searched, seized or interrogated except as provided by Act. No person shall be punished, placed under preventive restrictions or subject to involuntary labor except as provided by Act and through lawful procedures. Warrants issued by a judge through due procedures upon the request of a prosecutor shall be presented in case of arrest, detention, seizure or search."

In terms of the scope of due process, both substantive and procedural due process components are recognized by the Supreme Court of the United States.[3] Unsurprisingly, greater emphasis is put on the procedural due process aspects of judicial proceedings in that context. However, due to the potential for the loss of liberty if convicted, there is a substantial need for due process in criminal cases because of the potential for the sovereign coercive is bringing its power to bear on individuals.[4]

This section will discuss peculiar due process issues in investigation and prosecution of cybercrimes and also review relevant arguments linked with the Budapest Convention.

II. Due Process in Investigation & Prosecution of Cybercrimes

General due process requirements apply when investigating and prosecuting crimes include, *inter alia,* the right of the defendant to confront his or her accuser, the right to counsel and the right to a speedy trial. As mentioned, this section focuses on more specific and frequent cybercrime-related issues, notably **(A)** imbalance of obtaining evidence and **(B)** search and seizure.

A. Obtaining Evidence

Issues of the admissibility of evidence in court, such as the requirements of authenticity, integrity and reliability of digital evidence, have already been discussed (*see* sections 2 C and 2 D, above). From a procedural due process point of view, even though cybercriminals operate in a sophisticated and cross-border environment, there can still be a power imbalance between investigative agencies and defendants: compared to individual defendants, investigators and prosecutors have more negotiating power, especially when searching and securing evidence.

Moreover, once an investigation reaches the prosecutorial phase, there is likely more inculpatory evidence in favor of the state than exculpatory evidence in favor of the defendant. Yet justice systems, beholden to the rule of law, need to be fair and neutral.

B. Search & Seizure

If the search and seizure violates the criminal procedure law and/or the constitutional law in principle, the evidence that is seized ought to be excluded from evidence.

In the United States, there are various federal statues which set a limit on the investigatory power:

- **Wiretap Act (19 USC § 2510):** This Act governs the seizure of the content of digital messages. It places a general prohibition on intercepting the contents of wire, oral or electronic communications. Violation of the Act can cause criminal punishment or/and civil damages. Only by an order of a federal judge can interception be permitted or justified.[5]
- **Pen Register and Trap and Trace Statue (18 USC § 3121):** This statute governs the seizure of real-time traffic data—dialing, routing, addressing and signaling information provided by a communications service provider. It generally prohibits the nonconsensual real-time acquisition of non-content information by any person by wire or electronic communication unless a statutory exception applies.[6]
- **Electronic Communications Privacy Act (18 USC § 2701):** This Act protects individuals' privacy and proprietary interests, which applies when law enforcement officials seek to obtain records about a customer or subscriber from a communication service provider.[7] Specifically, it looks to protecting stored communications.
- **Fourth Amendment of US Constitution:** This constitutional provision—part of the original set of amendments to the US Constitution, collectively known as the Bill of rights—is construed as prohibiting the search or seizure of an individual or their property, unless a warrant is first obtained from a judge or the circumstances fall within very limited number of situations where a warrant is deemed unnecessary.[8]

The United Kingdom has recently broadened the surveillance capacities of its law enforcement authorities, relying on a so-called "double-lock" procedure to limit potential government abuse:

In the United Kingdom, the Investigatory Powers Act 2016[9] significantly expanded the surveillance power of law enforcement, granting authorities unprecedented surveillance powers to access private data of individuals.[10] The controversial law[11] was advanced to support law enforcement agencies in prevention and prosecution of modern crimes.[12] Specifically, the Act requires communication service providers to preserve their customers' data for a year. In addition to the data retention obligations, businesses are legally mandated to remove any encryption that interferes with warrants. Moreover, the Act enables authorities to intercept and store all forms of data, even

where techniques include hacking and surveilling individuals' electronic devices.[13] Lastly, bulk-data collection is permitted for the purpose of acquiring intelligence relating to individuals beyond the UK territorial border, as long as a warrant is issued.

Oversight for the Act, and thus for the releasing of these vast and intrusive powers, is controlled through what is called a "double-lock"; that "double-lock" requires a warrant to be approved by both government ministers and the specially-created judicial panel called the Investigatory Powers Commission.[14] In case of urgency, a warrant can be issued without the Commission's involvement insofar as it is subject to review by the Commission within three working days.[15] Already a heavily surveilled population,[16] UK authorities are now, along with Chinese and Russian authorities, a "global leader" in bulk surveillance of its citizens.[17]

Among other jurisdictions, Korean law guarantees the right of the defendant to participate in the search and seizure of an information storage device such as a computer. For example, Articles 121 & 122 of the Korean Criminal Procedure Act provide as follows:

> "A prosecutor, the criminal defendant, or his/her defense counsel may be present when a warrant of seizure or of search is being executed. Where a warrant of seizure or of search is to be executed, the persons listed in the preceding Article shall be notified of the date and place of execution in advance. [...T]his shall not apply in cases where a person prescribed in the preceding Article, clearly expresses his/her will in advance to the court that he/she does not desire to be present or in case of urgency."

The Korean Supreme Court has strictly interpreted the above provisions, ruling that the seizure and search procedure of information storage device was illegal for failing to guarantee the participation right of those subject to seizure in the review procedure conducted after taking out information storage device.[18]

Case 4.1: United States v. Ulbricht ("Silk Road") (USA)[19]

On 29 May 2015, a Manhattan federal court somewhat controversially[20] sentenced Ross William Ulbricht to life in prison in connection with his operation and ownership of Silk Road between January 2011 and October 2013.[21] Silk Road was a hidden "darkweb" website that enabled users to buy and sell illegal drugs and other unlawful goods and services anonymously and beyond the reach of law enforcement;[22] the black market was designed "as an online utopia beyond law enforcement's reach".[23]

During the court proceedings, Ulbricht claimed that, although he had initially been involved in the site, and although he even averred that illicit activities may have been conducted

on the site, he had sold this stake and was no longer involved in Silk Road. With regard to the evidence that the state presented, the defense argued that government surveillance of Ulbricht's online accounts was overboard and amounted to a violation of defendant's constitutional, Fourth Amendment rights, which protects against undue search and seizure.[24] It was further argued that evidence favorable to the defendant regarding corrupt officials had been improperly suppressed and tainted the case and evidence.

Ulbricht appealed his conviction saying, "The court abused its discretion and denied Ulbricht his Fifth and Sixth Amendment rights to due process, the right to present a defense, and a fair trial by (A) precluding the defense from using at trial the evidence relating to DEA Special Agent Carl Force's corruption; (B) refusing to order the government to provide additional discovery and 'Brady' material regarding corruption; and (C) denying Ulbricht's motion for new trial based on additional post-trial disclosures regarding Force and another corrupt law enforcement agent involved in the Silk Road investigation."[25]

While Ulbricht lost his appeal in May 2017,[26] the arguments made are ones that might well be raised by defendants charged with cybercrimes.

III. Budapest Convention & Due Process

A general discussion of multilateral and international agreements in cybercrime can be found in section 4 B, below. While the Budapest Convention is discussed in more detail in that section, it is worth noting here that the Convention is alone among multilateral and international instruments in specifically addressing safeguards and due process issues. That said, the provisions of the Convention show the inherent tension among information gathering and investigative powers and requirements of due process. With regard to due process safeguards, the Convention has specific provisions on **(A)** general conditions and safeguards, **(B)** expedited preservation of stored computer date and search and seizure of stored computer data and **(C)** expedited preservation and partial disclosure of traffic data and expedited disclosure of preserved traffic data.

A. Safeguards

Article 15 of the Budapest Convention provides, *inter alia,* that domestic law shall implement "conditions and safeguards [... that] provide for the adequate protection of human rights and liberties". Although binding on its Member States, a treaty mechanism alone as a source of due process is insufficient without local law implementation.[27] To that end, Member States are bound by the Convention to transpose implementing provisions into their national laws.

B. Treatment of Stored Computer Data

The safeguards referred to in article 15 are balanced against, for example, articles 16 and 29 of the Convention which provide, respectively, that "Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system",[28] and that "[a] Party may request anther Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data."[29] How the investigative authorities of each Member State carry out effective search and seizure will also be a matter of national law, and the duration of evidance preservation could be confined since the purpose of a preservation order is to get enough time to carry out legal procedures such as issuing warrant.[30]

C. Treatment of Traffic Data

Similarly, articles 17 and 30 of the Budapest Convention set up tools to secure expedited preservation of traffic data and require traffic data to be disclosed to the investigation agency so that routes of transmission can be identified.

Article 17 provide that "Each Party shall adopt […] such legislative and other measures as may be necessary to:

> "(a) Ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and
>
> "(b) Ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted."[31]

Article 30 complements this language:

> "[T]he requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted."[32]

Conclusion

For a vibrant online community that fosters robust economic growth and development to exist, a "trust" environment must be nurtured and developed. As discussed, doing as much means, first, building secure systems, and creating the enabling environment—legal and institutional—that empowers authorities to combat cybercrime, be it from domestic or international sources.

However, securing cyber systems against crime and empowering government authorities is only part of the puzzle: for the ecosystem to thrive, it must be trusted by users in larger sense than for commercial purposes and the sort. The cyberworld must be a place in which individuals and communities desire to constructively and completely engage, and where they are comfortable expressing themselves. To that end, protections safeguarding individual rights and guarding against government abuse or overreach must be built in. Doing so requires ensuring that due process rights are respected, which means that defined procedures—with limits and controls—must be developed for those occasions where authorities seek to obtain evidence or engage in search and seizure. Among international instruments, the Budapest Convention alone includes robust safeguards, which are to be transposed into national substantive law by each Member State.

The next section continues this discussion, looking to the government's responsibility to assure the protection of data and to guarantee the right to communicate. In creating and keeping cyberspace safe and secure, human rights must also be respected and protected.

B. Data Protection & the Right to Communicate

Table of Contents

Introduction

Up to this point, the Toolkit has focused on ways to effectively combat cybercrime, with only the last section looking to expand the responsibilities of the government to include factors requisite for create a "trust" environment (*see* section 4 A, above). It has done so from a series of different perspectives, including those of protecting not only ICT networks and systems, but also protecting the content and personal data stored therein. However, as the internet becomes an increasingly important platform for not only commercial but also non-commercial purposes, and as societies become increasingly dependent upon the interconnectivity that cyberspace allows, governments have increasingly deployed powers to seek to secure it. Such security must be balanced with the rights of individuals in the community, and must not hamstring the internet as a flexible, decentralized, open and neutral platform. As such, it is important to ensure that, in addition to providing the kind of security that comes from an effective cybercrime regime, the power of the state is deployed in a measured manner that effectively balances security with basic human rights. That balance perhaps most notably applies to assuring the protection of users' data and their right to privacy which also assures both access to information and freedom of expression.[1] At the same time, the state is obliged to defend basic human rights by investigating those who violate the privacy of others' communications, personal data and the like.

Apart from having a grounding in international law, assuring respect for human rights in the cybercrime context is a matter of good policy.[2] Recent scholarship squarely identifies and makes the link between advancing rights of privacy and expression in the ICT context, on the one hand, to achieving development objectives, on the other.[3] It is generally accepted that free speech facilitates the creation of a so-called "marketplace of ideas"; in turn, free speech encourages growth, be it commercial, intellectual, artistic or political.[4] Balancing stakeholder interests of security and of stability, on the one hand, and promoting human rights, on the other, is essential to promoting the enabling "trust" environment needed for building a digitally interconnected cyber-society (*see* section 4 A, above).[5]

Just as society has expanded into cyberspace, so, too, have authorities, and law enforcement in particular, expanded into and taken advantage of technological developments. Law enforcement and national security agencies need access to ICT, and therefore utilize "wiretapping" (and similar targeted-surveillance techniques), call center data registry and other metadata reporting measures to investigate criminal activity.[6] While the use of any and all of these tools poses certain privacy concerns, their deployment with appropriate safeguards, including the external seeking of appropriate and independent authorization, has largely resulted in the building of secure, commercially robust, internet-based societies where human rights still manage to flourish. Fundamental principles of "legality", "necessity" and "proportionality" feature in this debate and in creating such a "trust" environment that is so central to building a robust cyber society (*see* section 1 B, above).

One of the key drivers in the digital economy is the flow of data, much of which is personal data. Indeed, the amount of that data has increased by an estimated ninety percent in the last few years.[7] This trend has in part been fueled "big data" applications for monitoring and manipulating data.[8] Big data refers to both structured and unstructured data which is both of such a volume and which is also communicated at such a high rate that it is difficult to process using traditional database and software techniques.[9] Big data applications can be found in both the public and private sectors. While probably most commonly associated with private sector applications (such as Facebook and Google), it is conceivable that these same, big-data analytical techniques could be used in the fight against cybercrime; if so, attention would need to be paid to the prospect of intrusions into individuals' privacy.

The issue goes beyond simply having and enforcing national laws protecting personal data. As is the case with cyberspace in general, data flows (whether legitimate or not) are global. As such, in order to be effective, privacy regimes need to both enable and further facilitate legitimate internet usage, as well as to assure individuals' rights in the case of combatting cybercrime.

I. Applicable International Law & Good Practice

First, before exploring the application of any rights in detail, it merits clarifying that guaranteeing the protection of human rights on the internet has been recognized in recent years through a series of statements emanating from the United Nations.

Beginning in 2011, in a report to the to the ***UN Human Rights Council*** (UNHRC) on the promotion and protection of the right to freedom of opinion and expression on the internet, Special Rapporteur, Frank La Rue, concluded that "states [are] providing inadequate protection of the right to privacy and data protection".[10] In the following year, the UNHRC "affirmed that people have the same rights online that they have offline […] in particular [regarding] freedom of expression".[11]

In 2016, the UNHRC reaffirmed "the importance of promoting, protecting and enjoying human rights on the internet, including privacy and expression".[12] In June 2016, the UN General Assembly subsequently adopted a Resolution announcing the following:

> "Calls upon all States to address security concerns on the Internet in accordance with their international human rights obligations to ensure protection of freedom of expression, freedom of association, privacy and other human rights online, including through national democratic, transparent institutions, based on the rule of law, in a way that ensures freedom and security on the Internet so that it can continue to be a vibrant force that generates economic, social and cultural development [....]"[13]

With the question of government responsibility for adhering to human rights standards in implementing cybersecurity born in mind, the UNHRC concluded as follows:

> "Decides to continue its consideration of the promotion, protection and enjoyment of human rights, including the right to freedom of expression, on the Internet and other information and communication technology, as well as of how the Internet can be an important tool for fostering citizen and civil society participation, for the realization of development in every community and for exercising human rights, in accordance with its programme of work."[14]

Second, and specifically in the cybercrime context, frameworks for generally safeguarding rights while also providing security exist, the most notable of which is perhaps that promulgated by article 15 of the ***Budapest Convention.*** That basic framework provides as follows:

> (1) Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall

> provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.
>
> (2) Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia,* include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.
>
> (3) To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.[15]

The ***Explanatory Report to the Budapest Convention*** discusses the principle of proportionality referenced in article 15.1, as follows:

> "[A]nother safeguard in the Convention is that the powers and procedures shall incorporate the principle of proportionality. Proportionality shall be implemented by each Party in accordance with relevant principles of its domestic law. For European countries, this will be derived from the principles of the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, its applicable jurisprudence and national legislation and jurisprudence, that the power or procedure shall be proportional to the nature and circumstances of the offence. Other States will apply related principles of their law, such as limitations on over breadth of production orders and reasonableness requirements for searches and seizures."[16]

Thus, the basis for assuring human rights, even as cyberspace is secured, is soundly and explicitly provided for in international law. The rest of this section delves in more detail into the concrete application of privacy rights and data protection, as well as the right to communicate (*i.e.,* freedom of expression and the right to access to information). As data protection and the right to communicate are closely interlinked, they are treated together in this section; that said, they also have different features that need to be understood on their own.

II. Data Protection & Privacy

The discussion around data protection and privacy merits **(A)** an introductory discussion of security-privacy debate that can be used to set up a fuller discussion of **(B)** good practices in legal instruments guaranteeing data protection and privacy.

A. The Security-Privacy Debate

Data protection speaks to the provision of reasonable assurances that individuals' rights regarding their personal data and privacy are observed and protected. It extends not only to those under investigation and prosecution but also to potentially innocent third parties who may become involved, or whose data might be touched upon.

The policy, legal and technical differences between "security" and "privacy" merit clarifying at this stage. There are a variety of ways in which the two terms can be understood. Generally speaking, "security" can be understood as a set of technological measures that mediate access to personal data stored or transmitted via ICT systems or networks, while "privacy" is the normative framework for allocating who has access to that data, including the right to alter any of it.[17] Some posit the two values as running counter to each other, a conception out of which the overly-simplistic argument "if you've got nothing to hide, then you've got nothing to worry about surveillance" emerges.[18]

Others posit that the two are not in the same plane, and that there is a false trade-off between privacy and security that has resulted from an incorrect framing of the debate as a zero-sum game in which one value is pitted against the other.[19] Still others posit that implementation of good data protection principles is not merely a matter of securing human rights but actually contributes to reducing certain kinds of cybercrime.[20] The concern here is how the security aspects of ensuring an effective cybercrime regime impact upon privacy of an individual's data.

B. Legal Instruments Guaranteeing Data Protection & Privacy

The right to privacy can be found in both article 12 of the ***Universal Declaration of Human Rights*** (UDHR) and in the ***International Covenant on Civil and Political Rights*** (ICCPR).

Article 12 of the UDHR provides as follows:

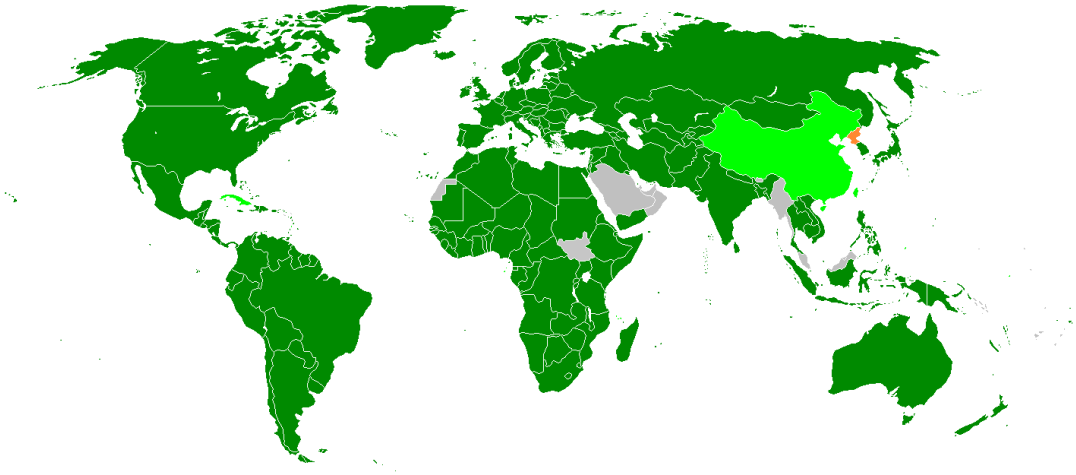
> "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."[21]

Similarly, article 17 of the ICCPR provides as follows:

> (1) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, or correspondence, nor to unlawful attacks on his honour and reputation.
>
> (2) Everyone has the right to the protection of the law against such interference or attacks.[22]

Importantly, these rights are not absolutes, and, as also reflected in article 15.3 of the Budapest Convention, are subject to certain limits.

Figure 4.1: Current Membership in the ICCPR[23]



While rights to privacy and expression have evolved over time over the past three hundred years[24], and, when set down in 1948 in the case of the UDHR, and in 1966 in the case of the ICCPR, were certainly not drafted with the internet or cybercrime in mind, the UN Human Rights Council recently reaffirmed the importance of promoting, protecting and enjoying human rights on the internet, including privacy and expression.[25] In 2013, the UN General Assembly adopted a Resolution, introduced by Brazil and Germany, on the Right to Privacy in the Digital Age.[26] Today, the UN Conference on Trade and Development (UNCTAD) reports that 107 countries have privacy laws in place, sixty-six of which are developing countries.[27]

Regional initiatives have built upon these international instruments. In Europe, the ***European Convention on Human Rights*** (and related caselaw) sets the legal base for understanding and guaranteeing fundamental human rights, including those to privacy and expression. While there are a number of other relevant instruments, the ***Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*** (Convention 108)[28] is the single most significant

instrument. Opened for signature on 28 January 1981 and entering into force on 1 October 1985, the Convention was the first legally binding international instrument in the data protection field. Under the Convention, Parties are required to take the necessary steps in their domestic legislation to apply the Convention's principles ensuring respect for the fundamental human rights of all individuals with regard to processing of personal data.

Convention 108 is open for accession by any State, regardless of geographic location, or of CoE membership. Uruguay (in 2013) and Mauritius (in 2016) were the first non-European countries to become Parties to the Convention. Today, the Convention has fifty Parties, seven of which are non-Members of the Council of Europe.[29] It is indicative that countries seeking to implement the Budapest Convention on Cybercrime also show strong interest in Convention 108, or are enacting their own domestic data protection regimes.[30]

An ***additional Protocol to Convention 108*** (Convention 181) covers supervisory authorities and transborder data flows.[31] The additional Protocol requires Parties to set up supervisory authorities and, among other things, that those authorities exercise their functions in "complete independence".[32] That independence is understood as an element central to the effective protection of individuals with regard to the processing of personal data.[33]

Still in the European context, a related soft law instrument is CoE's ***Recommendation R(87) 15 on data protection in the police sector.***[34] Bearing in mind the "sectoral approach" taken to data protection up till that time,[35] the Recommendation puts forth principles that might guide Member States in their domestic law and practice. Those basic principles include address data control and notification; collection; storage; usage by police; communication between public and private bodies; publicity and right to access, rectify and appeal data; length of storage and updating data; and data security.[36] Although soft law, the Recommendation, created on 17 September 1987, has been widely adopted across Europe "to an extent that many European states *prima facie* already regulate[d] police use of personal data in a way comparable but not necessarily identical to that envisaged in the European Commission's proposal […] for a Directive" on the same matter.[37] While not obviating the utility and advantages of having a suitable new binding legal instrument, the high degree of *de facto* adherence highlights, first, the degree of influence that even soft law can have, and, second, the degree to which states are both working and able to comfortably balance security and privacy obligation even in the police context.

An additional source of international good practice of the principal features of a data protection/ privacy regime can be found in the Organization for Economic Cooperation and Development (OECD) ***Guidelines for the Security of Information Systems and Networks*** ("OECD Guidelines").[38] The Guidelines provide measures direction in ensuring the quality of data collected; the scope of the purposes for which data may be collected and used; the setting of strict limits on the use of collected data; the setting of safeguards in terms of data collection, storage and usage; and covers rights of data subjects to correct or erase erroneous data.

Box 4.1: Basic Information Security Principles from OECD Guidelines

Collection Limitation Principle: There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Data Quality Principle: Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

Purpose Specification Principle: The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use Limitation Principle: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the purpose specification principle except: a) with the consent of the data subject; or b) by the authority of law.

Security Safeguards Principle: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

Openness Principle: There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

Individual Participation Principle: Individuals should have the right:

(a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to them;

(b) to have communicated to them, data relating to them (i) within a reasonable time; (ii) at a charge, if any, that is not excessive; (iii) in a reasonable manner; and (iv) in a form that is readily intelligible to them;

(c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and

(d) to challenge data relating to them and, if the challenge is successful to have the data erased, rectified, completed or amended.

Accountability Principle: A data controller should be accountable for complying with measures which give effect to the principles stated above.

Collectively, these international and regional instruments, as well as the principles and guidelines, provide a rich source of international good practice for how to balance security with data protection and privacy. The flexible, open and decentralized nature of the internet augurs in favor of a principles-based approach (with notion of proportionality at its core) that balances state interventions and intrusions with individual human rights. As the internet functions on the basis of the creation of a "trust" environment, it is essential that such considerations and be weighed openly.

C. The Special Place for Anonymity

Anonymity can be seen as an essential component of protecting privacy on the internet.[39] Not infrequently, this same anonymity is also highly problematic for public safety, due in part to legal and technical reasons. Particularly in the digital context, those same basic human rights protections that make the internet such a compelling and exciting tool for development and social advancement can also lead to problems of authentication in general, and attribution—that is, the connecting of a criminal actor to the act perpetrated—in particular. From a technical perspective, encryption is perhaps the most obvious issue.[40] From a larger, legal perspective, particular difficulties exist where there is a divergence of legal frameworks, especially in light of a still-evolving MLAT framework. The latter obstacle is in part overcome by shared adherence to multilateral instruments, such as the Budapest Convention, which, among other things, creates such a framework.[41]

The issue of privacy and data protection in the context of surveillance, especially "mass" surveillance, is a particularly thorny issue.[42] While the topic of "surveillance", generally, is beyond the scope of the Toolkit, surveillance is an important tool for law enforcement in investigating crime, including cybercrime. The technological advances that have enabled cybercrime to expand have also enabled expanded surveillance tools and methodologies. All of these developments have resulted in unresolved questions of what are, and how to define, the appropriate limits on the collection of data relevant to an investigation.

III. The Right to Communicate

The "right to communicate", as already discussed, speaks to the complementary rights of "freedom of expression" and "access to information" (*see* section 1 C, above). Communication, one of the

most basic of human rights and of human behaviors,[43] is addressed in the UDHR and is more fully expressed in the ICCPR, as described below. These rights are also reflected in a number of regional instruments.[44]

The UDHR provides in Article 19 as follows:

> "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."

The ICCPR goes somewhat further, providing a specific framework for addressing the balance of security versus rights. The ICCPR not only provides for the right itself (articles 19.1 & 19.2), but also provides factors that should be considered in "balancing" this right with other governmental prerogatives (article 19.3):

> (1) Everyone shall have the right to hold opinions without interference.
>
> (2) Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.
>
> (3) The exercise of the[se] rights […] carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:
>
> (a) For respect of the rights or reputations of others; [and]
>
> (b) For the protection of national security or of public order ("*ordre public*"), or of public health or morals.

Among human rights, the right to communicate is a particularly interesting one, as it is not only substantively fundamental (the right to communicate is a right in itself), but it is also procedurally fundamental (as it also an "enabler" of other fundamental rights). In addition, freedom of expression and access to information are both and equally essential to the enjoyment of economic, social and cultural rights, such as the right to education and the right to partake in cultural life or benefits of scientific progress, as well as civil and political rights, such as the rights to freedom of association and assembly. In this sense, the right to communicate is also part of the "trust"

equation discussed above; illegitimate efforts to repress expression in the name of security could have deleterious effects on internet usage for legitimate purposes.[45]

The internet thrives on the open exchange of information—that is, the so-called "marketplace of ideas"—which, in equal measure, requires both access to information and freedom of expression.[46] For example, innovation, and the incentive to innovate, depends on striking an appropriate balance between providing access to information, on the one hand, and rewarding inventors by protecting intellectual property rights, on the other.

Rapid cyber and ICT developments have allowed the internet to be a particularly powerful driver of economic, social and even political changes. Those changes have been accompanied by a wide array of legal and regulatory initiatives, some of which indirectly or even unintentionally place limits on the right to communicate but which nonetheless may have a chilling effect on expression.[47] For example, governments frequently regulate access to certain content in order to reduce criminal activity. In other circumstances, it is possible that governments have incidentally criminalized online expression by failing to keep laws regulating broadcasting current with technological developments.[48] A recent study by UNESCO on the issue of preserving online freedom of expression advocated promoting a balance between security and expression. According to that study, governments should take a pragmatic approach that minimizes online restrictions yet which addresses issues arising out of legitimate societal values.[49] Such an approach helps to ensure a vibrant future of the internet, preserving its role as a place for the exchange of ideas that has made it such a unique and powerful platform for economic, social and political progress.

Conclusion

In designing and implementing legal frameworks to combat cybercrime, states should reconcile the different interests that are to be protected. Although data protection/privacy and security may be construed as competing, even mutually-exclusive concerns, there is a rich body of international good practices showing that, at minimum, the privileging of one need not result in the significant diminution of the other. In any case, where one right is curtailed, it should be done on the basis of the principle of proportionality. If a state compiles, stores, uses or discloses personal information—for example, in a police register—, such interference or intrusion into a person's private life should meet certain conditions under law, that respect due process and re-enforce the "trust" principle by being both proportionate to the legitimate aims pursued and necessary. To ensure that the internet's full potential is reached, and in order to avoid having a chilling effect on communication—both in personal expression, and in the seeking and acquiring of information—, the laws and their application, whether inadvertently or purposefully, must be kept open and pragmatic.

End Notes

Referenced in: § A. Introduction & Due Process

1. *See* WDR, *supra* § 1 A, note 10, at 222 *et seq.*

2. Although these notions have been most broadly developed in common law traditions, similar notions are at play in the civil law tradition in, for example, the concept of *respect pour l'Etat de droit* ("respect for the state of the law"). *See, e.g., "Traités et Affaires institutionnelles: Respect de l'état de droit – La Commission, soutenue par une majorité du Parlement européen, maintient la pression sur Varsovie,"* EuropaForum, (13 Sept. 2016), at http://www.europaforum.public.lu/fr/actualites/2016/09/pe-pologne-etat-de-droit/index.html. At the international level, these notions have been evoked in, for example, the ICCPR (Art. 14) and in the ECHR (Art. 6).

3. Miriam F. Miquelon-Weismann, "The Conversation on Cybercrime: A Harmonized Implementation of International Penal Law: What Prospects for Procedural Due Process?," John Marshall Journal of Computer & Information Law, Vol. 23 (2005), p. 355; *Schriro v. Summerlin,* 124 S. Ct. 2510, 2523 (2004).

4. Michael Farbiarz, "Accuracy and Adjudication: The Promise of Extraterritorial Due Process," Columbia Law Review, Vol. 116, Issue 3, (Apr. 2016), pp. 636–37.

5. Chief Judge B. Lynn Winmill, David L. Metcalf & Michael E. Band, "Cybercrime: Issues and Challenges in the United States," Digital Evidence & Electronic Signature Law Review, Vol. 7 (2010), p. 31.

6. *Ibid.*

7. *Ibid.*, at 32.

8. *Ibid.*

9. *See* United Kingdom: Investigatory Powers Act 2016 [hereafter, "UK Investigatory Powers Act"], Ch. 25, at: http://www.legislation.gov.uk/ukpga/2016/25/pdfs/ukpga_20160025_en.pdf. *See also,* "Investigatory Powers Act 2016", UK Parliament, at http://services.parliament.uk/bills/2015-16/investigatorypowers.html.

10. Law enforcement authorities only need a "retention notice", not a warrant, which requires telecommunications operators to retain specified items of communications data for the period or periods set out in the notice (limited to twelve months). Although there are safeguards and matters that must be considered before the giving of a retention notice, the procedural threshold is lower than that for a traditional warrant. *See* UK Home Office, *Investigatory Powers Bill: Explanatory Notes to the Investigatory Powers Bill as brought from the House of Commons on 8 June 2016 (HL Bill 40),* para. 232, at https://www.publications.parliament.uk/pa/bills/lbill/2016-2017/0040/17040en.pdf.

11. Ewen MacAskill, "'Extreme Surveillance' Becomes UK Law with Barely a Whimper," Guardian, (19 Nov. 2016), at https://www.theguardian.com/world/2016/nov/19/extreme-surveillance-becomes-uk-law-with-barely-a-whimper.

12. Andrew Griffin, "Investigatory Powers Act Goes into Force, Putting UK Citizens under Intense New Spying Regime," Independent, (31 Dec. 2016), at http://www.independent.co.uk/life-style/gadgets-and-tech/news/investigatory-powers-act-bill-snoopers-charter-spying-law-powers-theresa-may-a7503616.html.

13. Emma Woollacott, "UK Joins Russia and China in Legalizing Bulk Surveillance," Forbes, (16 Nov. 2016), at https://www.forbes.com/sites/emmawoollacott/2016/11/16/uk-joins-russia-and-china-in-legalizing-bulk-surveillance/#718b3a2b58ca

14. UK Investigatory Powers Act, *supra* note 9, at Art. 23.

15. *Ibid.*, at Art. 24.

16. *See, e.g.,* David Barrett, "One Surveillance Camera for Every 11 People in Britain, Says CCTV Survey," Telegraph, (10 Jul. 2013), at http://www.telegraph.co.uk/technology/10172298/One-surveillance-camera-for-every-11-people-in-Britain-says-CCTV-survey.html; Paul Lewis, "You're Being Watched: There's One CCTV Camera for Every 32 People in UK," Guardian (2 Mar. 2011), at https://www.theguardian.com/uk/2011/mar/02/cctv-cameras-watching-surveillance.

17. Griffin, *supra* note 12.

18. Korean Supreme Court, 2011MO1839 (16 Jul. 2015), *en banc* ruling.

19. *Ulbricht, supra* § 2 B, note 111. This case is highlighted above as an exposé of the diversity of technology and its enabling effect on cybercrime. *See supra* § 2 B, box 2.6.

20. Andy Greenberg, "Judges Question Ross Ulbricht's Life Sentence in Silk Road Appeal," Wired, (6 Oct. 2016), at https://www.wired.com/2016/10/judges-question-ulbrichts-life-sentence-silk-road-appeal/.

21. *See* US Dept. of Justice, "Ross Ulbricht, A/K/A 'Dread Pirate Roberts,' Sentenced in Manhattan Federal Court to Life in Prison," Press Release, (29 May 2015), at https://www.justice.gov/usao-sdny/pr/ross-ulbricht-aka-dread-pirate-roberts-sentenced-manhattan-federal-court-life-prison. *See also* Andy Greenberg, "Silk Road Creator Ross Ulbricht Sentenced to Life in Prison," Wired, (29 May 2016), at https://www.wired.com/2015/05/silk-road-creator-ross-ulbricht-sentenced-life-prison/.

22. Joshua Bearman & Tomer Hanuak, "The Rise & Fall of Silk Road," Wired, (May 2015), at https://www.wired.com/2015/04/silk-road-1/.

23. Greenberg, *supra* note 20.

24. US Constitution, IV Amend.: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

25. *See, e.g.,* John Zorabedian, "Ross Ulbricht Appeals Silk Road Conviction—Did He Get a Fair Trial?," Naked Security, (18 Jan. 2016), at https://nakedsecurity.sophos.com/2016/01/18/ross-ulbricht-appeals-silk-road-conviction-did-he-get-a-fair-trial/.

26. *See United States v. Ulbricht*, No. 15-1815, (2d Cir. 2017), at https://cases.justia.com/federal/appellate-courts/ca2/15-1815/205494850/0.pdf?ts=1496418409. Also *see*, Greenberg, *supra* note 20; Andrew Blake, "Attorney for Silk Road Mastermind Ross Ulbricht Challenges Conviction in Federal Appeals Court," Washington Times, (7 Oct. 2016), at http://www.washingtontimes.com/news/2016/oct/7/appeals-court-hears-case-against-ross-ulbricht-con/.

27. Miquelon-Weismann, *supra* note 3, at 356–57.

28. Budapest Convention, *supra* § 1 B, note 32, at Art. 16.

29. *Ibid.*, at Art. 19.

30. Hyun Wook Chun & Ja Young Lee, "Convention on Cybercrime and Due Process of Law: on Preservation and Partial Disclosure of Stored Data," Korean Criminological Review, Vol. 25, Issue ii, (2014), p. 98.

31. UK Investigatory Powers Act, *supra* note 9, at Art. 17.

32. *Ibid.*, at Art. 30.

Referenced in: § B. Data Protection & The Right to Communicate

1. A full exposition of privacy/data protection and access to information/ freedom of expression is beyond the scope of the Toolkit. In its limited discussion, while the Toolkit uses the terms "privacy" and "data protection" interchangeably, both terms are intended to refer to the protection of digital data about a person, and not to other normative constructs about what privacy might mean. In addition, there is very little in the literature (a few sources appear in this chapter) specifically about the intersection of the security that comes with a cybercrime regime and the tensions that security may place on rights such as privacy and the right to communicate.

2. *See, e.g.,* Recent jurisprudence from both the Court of Justice of the European Union (CJEU) and the European Court of Human Rights (ECtHR) support striking this balance. In: *Digital Rights Ireland Ltd v. Ireland* and *Seitlinger and Others,* joined cases C-293/12 & C-594/12 (8 Apr. 2014) [hereafter, *"Seitlinger"*], the CJEU ruled the EU Data Retention Directive to be in violation of the EU Charter of Fundamental Rights. Similarly, in: *S and Marper v. United Kingdom,* the ECtHR, using a proportionality analysis, found the United Kingdom to be in breach of Article 8 of the European Convention on Human Rights, holding that the long-term retention of both fingerprints and DNA samples interfered with an individual's right to privacy. *S and Marper v. United Kingdom,* 30562/04 [2008] ECtHR 1581 (4 Dec. 2008).

3. WDR, *supra* § 1 A, note 10, at 222 *et seq.* In particular, the WDR notes "[…] that getting the data protection and privacy piece of the puzzle right is, together with cybersecurity, a key element in engendering trust in and confidence in use of the internet" *Ibid.,* at page p. 227.

4. *See e.g,* Stanley Ingber, "The Marketplace of Ideas: A Legitimizing Myth," Duke Law Journal, Vol. 33 (1987), p. 1.

5. WDR, *supra* § 1 A, note 10, at p. 222 *et seq.* The WDR notes that "getting the data protection and privacy piece of the puzzle right is, together with cybersecurity, a key element in engendering trust in and confidence in use of the internet". *Ibid.,* at p. 227.

6. Data about a communication, as opposed to the *content* of the communication. The aggregation of information commonly referred to as "metadata" may give an insight into an individual's behavior, social relationships, private preferences and identity that go beyond even that conveyed by accessing the content of a private communication. As the CJEU recently observed, communications' metadata "taken as a whole may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained." *See, e.g., Seitlinger, supra* note 2.

7. Science News, "Big Data, for Better or Worse: 90% of World's Data Generated Over Last Two Years," Science Daily, (22 May, 2013), at https://www.sciencedaily.com/releases/2013/05/130522085217.htm.

8. *See Seitlinger, supra* note 2.

9. Vangie Beal, "Big Data," Webopedia, at http://www.webopedia.com/TERM/B/big_data.html.

10. UN Human Rights Council, "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression," A/HRC/17/27 (16 May 2011), at http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf.

11. UN Human Rights Council, "The Promotion, Protection and Enjoyment of Human Rights on the Internet" (20th Session), A/HRC/20/L.13 (29 Jun. 2012), at http://ap.ohchr.org/documents/alldocs.aspx?doc_id=20280.

12. UN Human Rights Council, "The Promotion, Protection and Enjoyment of Human Rights on the Internet" (32d Session), A/HRC/32/L.20 (27 Jun. 2016), at http://daccess-ods.un.org/access.nsf/Get?Open&DS=A/HRC/32/L.20&Lang=E.

13. *Ibid.*

14. *Ibid.*

15. Budapest Convention, *supra* § 1 B, note 32.

16. Budapest Explanatory Report, *supra* § 1 D, note 14, at para. 251

17. *See* Derek Bambauer, "Privacy Versus Security," Journal of Criminal Law & Criminology, Vol. 103 (3) (2013), p. 667, at http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=7454&context=jclc

18. *See, e.g.,* Moxie Marlinspike, "Why 'I Have Nothing to Hide' Is the Wrong Way to Think about Surveillance," Wired, (13 Jun. 2013), at https://www.wired.com/2013/06/why-i-have-nothing-to-hide-is-the-wrong-way-to-think-about-surveillance/.

19. *See* Daniel J. Solove, *Nothing to Hide: The False Tradeoff between Privacy and Security,* (New Haven, Connecticut: Yale University Press, 2011).

20. *See* Maria Grazia Porcedda, *Data Protection and the Prevention of Cybercrime: The EU as an Area of Security?,* (Florence: European University Institute, 2012), at http://cadmus.eui.eu/handle/1814/23296.

21. UDHR, *supra* § 1 C, note 105, at Art. 12.

22. UN General Assembly, *International Covenant on Civil and Political Rights,* United Nations, Treaty Series, Vol. 999 (16 Dec. 1966), [hereafter ICCPR], p. 177, at https://treaties.un.org/doc/publication/unts/volume%20999/volume-999-i-14668-english.pdf.

23. UN Treaties Collection, "Status: International Covenant on Civil and Political Rights," United Nations, at https://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-4&chapter=4&lang=en

24. Early records of the foundational principles of individualism that form the basis of many of these rights first appeared in the French *Déclaration des droits de l'homme et du citoyen* ("Declaration of the Rights of Man and of the Citizen") adopted in 1789.

25. UN Human Rights Council, *supra* note 12, at para. 8 & 15.

26. UN General Assembly, "The Right to Privacy in the Digital Age," A/RES/68/167 (18 Dec. 2013), at http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/68/167.

27. *See* UN Conference on Trade and Development (UNCTAD), "Data Protection and Privacy Legislation Worldwide," United Nations, at http://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx

28. CoE, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data,* CETS No. 108 (28 Jan. 1981), at http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108

29. *Additional Protocol to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Regarding Supervisory Authorities and Transborder Data Flows,* CoE, CETS 181 (8 Nov. 2001), [hereafter, "Additional Protocol"], at http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/181.

30. For example, Morocco and Senegal have also requested accession to both treaties, and the Philippines have enacted domestic data protection laws.

31. Additional Protocol, *supra* note 29.

32. *Ibid.,* at Art.1.3.

33. *Ibid.*

34. *See* CoE Committee of Minsters, "Regulating the Use of Personal Data in the Police Sector," Recommendation No. R(87) 15 (17 Sep. 1987), at https://www.privacycommission.be/sites/privacycommission/files/documents/aanbeveling_87_15.pdf.

35. *See ibid.,* at Explanatory Memorandum to Recommendation No. R(87) 15, para. 2.

36. *Ibid.,* at Appendix to Recommendation No. R(87) 15, para. 1–8.

37. Joseph A. Cannataci & Mireille M. Caruana, *Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (T-PD),* (Strasbourg: CoE, 2014), at https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806ae16a

38. OECD, *Guidelines for the Security of Information Systems and Network,* (Paris: OECD, 2013), at https://www.oecd.org/sti/ieconomy/privacy-guidelines.htm. First promulgated in the 1980s, they were updated in 2013. The principles contained in the OECD Guidelines form the basis of most data protection/privacy laws around the world. *See, e.g.,* Françoise Gilbert, *Global Privacy & Security Law,* (Palo Alto, CA: Wolters Kluwer, 2017).

39. *See* UN Educational, Scientific, and Cultural Organization (UNESCO), "Keystones to Foster Inclusive Knowledge Societies: Access to information and Knowledge, Freedom of Expression, Privacy and Ethics on a Global Internet", (France: UNESCO, 2015), [hereafter, "UNESCO 1"], p. 43, at http://unesdoc.unesco.org/images/0023/002325/232563E.pdf.

40. For a fuller discussion of issues of encryption, *see supra* § 1 C.

41. For a fuller discussion of issues surrounding multilateral instruments and cross-border cooperation, *see supra* § 3 A.

42. *See generally,* Gus Hosein & Caroline Wilson Palow, "The Second Wave of Global Privacy Protection: Modern Safeguards for Modern Surveillance: An Analysis of Innovations in Communications Surveillance Techniques," Ohio State Law Journal, Vol. 74 (2013), p. 1071.

43. Many social scientists have spoken of the centrality of communication and communicating in what it means to be human. For instance, Aristotle called humans "social" or "political animals." *Politics,* Book 1, § 1253a. At the same time, James Baldwin, in relating the role of the novelist—an important form of communication—, has said that humankind "is not […] merely a member of a Society or a Group or a deplorable conundrum to explained by Science. He is […] something more than that, something resolutely indefinable, unpredictable. In overlooking, denying, evading his complexity […] we are diminished and we perish; only within the web of ambiguity, paradox, this hunger, danger, darkness, can we find at once ourselves and the power that will free us from ourselves." "Everybody's Protest Novel," in *Notes of a Native Son* (Boston, MA: Beacon Press, 1955).

44. For example, see Organization of American States (OAS), *American Convention on Human Rights* (22 Jan. 1969), Art. 13; CoE, *European Convention for the Protection of Human Rights and Fundamental Freedoms* (4 Nov. 1950), Art. 11; Organization of African Unity (OAU), *African Charter on Human and Peoples' Rights* (27 Jun. 1981), Art. 9; League of Arab States, *Arab Charter on Human Rights* (15 Sep. 1994), Art. 32; and Association of Southeast Asian Nations (ASEAN), *ASEAN Human Rights Declaration* (18 Nov. 2012), Art. 23.

45. The importance of the right to communicate is also inhered in the Sustainable Development Goals (SDGs). The SDGs recognize that sustainable development includes "public access to information and fundamental freedoms" as part of a wider goal (number 16) to: "Promote peaceful and inclusive societies for sustainable development, provide access to justice for all and build effective, accountable and inclusive institutions at all levels." *See* UN Sustainable Development, "Open Working Group Proposal for Sustainable Development Goals," UN Sustainable Development, at https://sustainabledevelopment.un.org/focussdgs.html

46. *See generally,* WDR, *supra* § 1 A, note 10, at p. 221.

47. *See, e.g.,* William H. Dutton, Anna Dopatka, Michael Hills, Ginette Law & Victoria Nash, *Freedom of Connection, Freedom of Expression; the Changing Legal and Regulatory Ecology Shaping the Internet,* (Paris: UNESCO, 2011) [hereafter, "UNESCO 2"], at http://unesdoc.unesco.org/images/0019/001915/191594e.pdf.

48. *See* UNESCO 1, *supra* note 39, at p. 41. In some cases, these inhibitory laws may have been designed for an analog media environment, making their application in the digital, internet context potentially problematic.

49. *See* UNESCO 2, *supra* note 47, at p. 79.

CHAPTER 5

International Cooperation

This chapter discusses both formal and informal aspects of international cooperation to combat cybercrime.

In this Chapter

A. Multilateral Instruments & Cross-border Cooperation

Table of Contents

Introduction

The global, trans-national, cross-border nature of cyberspace raises substantial jurisdictional issues (*see* section 2 E, above). Operating from a Westphalian nation-state concept of sovereignty, states—and their territorially-based cybercrime legislation—have been "plagued" by the boundary-defying fluidity of cyberspace and of cybercrime.[1] Further, different legal systems, with their own unique anomalies and idiosyncrasies, often present major obstacles to countries seamlessly and effectively fighting cybercrime across borders.

Although there are a number of offences that can be prosecuted anywhere in the world, regional differences play an important role in the effectiveness of combatting cybercrime. For example, different kinds of content are criminalized in different countries, which means that material that can lawfully be made available on a server in one country might be considered illegal in another (*see* section 2 E, case 2.3). The issue of convergence of legislation is highly relevant, as a large number

of countries base their mutual legal assistance (MLA) regimes on the principle of dual criminality (*see* section 2 A, above).[2] This means that, outside of mechanisms created by instruments such as the Budapest Convention (discussed below), if the "criminal" act for which the MLA request is only criminalized in one country that has acceded to the mutual legal assist stance treaty (MLAT), then the country being requested to provide assistance may not be authorized to do so.

Formal international cooperation aims at addressing three basic problems:

1. **Gap-fill national criminal laws** that are either incomplete (insofar as they do not deal with cybercrime) or that do not contemplate the kind of cross-border cooperation so often required in combatting cybercrime;
2. **Proffer procedural powers** where nations are not appropriately equipped to combat cybercrime; and
3. **Create enforceable MLA provisions** that would facilitate and expedite sharing and assistance in cybercrime matters.[3]

Effectively fighting cybercrime requires addressing each of these three areas, which demands both efforts at the national level, in developing an appropriate legal framework, and, at the international level, in creating mechanisms for the interoperability of those national frameworks. Failing to address both dimensions could result in the creation of safe havens for cybercriminals.[4] Formal international measures, mainly in the form of treaties, attempt to address these concerns by getting states to agree on how to address all of these issues.

Where cybercrimes are concerned, complete jurisdiction—that is, over the crime, the evidence and the alleged perpetrators (*see* section 2 E, above)—is frequently not obtained; as such, states must act beyond their territorial borders and, very frequently, cooperate with others in order to investigate and prosecute cybercrimes. Actions taken through the mechanisms of multilateral instruments, rather than by unilateral effort, are the most effective and important means of establishing extra-territorial jurisdiction over cybercrimes. Once a state has developed the appropriate legal framework for combatting cybercrime (*see* section 3 A, above), international cooperation is necessary to expand national territorially-based purview and to gap-fill, thereby building effective networks of interoperability that can function coherently and cohesively. That said, even where such formal instruments exist, effective implementation largely depends upon developing informal international relations, typically through additional mechanisms and interactions (*see* section 5 B, below).

Formal and informal modes of cooperation facilitate state consent for conducting foreign law enforcement investigations that affect a state's sovereignty. For example, law enforcement might access data stored extraterritorially where investigators use an existing live connection from a suspect's device, or where they use (lawfully-obtained) data-access credentials. Investigators may, on occasion, obtain data from extraterritorial ISPs through an informal direct request, although ISPs usually require due legal process (*see* section 2 C, case 2.11).

Formal international cooperation comes in various forms. The most targeted means are **(I)** cyber-specific multilateral treaties.[5] Globally, more than eighty states have signed and/or ratified one or more binding cybercrime instruments,[6] and many of those states have national cybercrime legislation.[7] More generally, formal yet non-cyber-specific mechanisms for international cooperation include **(II)** MLATs and **(III)** extradition treaties. These instruments set up frameworks for cooperation, encouraging or requiring states to look more closely at their own domestic legislation. The value of these instruments goes beyond their formal membership, however; notably, by providing a benchmark for states not bound to such instruments,[8] Including when taken together with other sources of good practice, these instruments provide important guidance when preparing, for example, model laws.[9]

I. Multilateral Treaties on Cybercrime

Five major cybercrime-specific, multilateral treaties exist: **(A)** the CoE's Budapest Convention, **(B)** the CIS Agreement, **(C)** the SCO Agreement, **(D)** the Arab Convention and **(E)** the AU Convention.

Despite these accomplishments and the fact that approximately eighty countries are party to one or more of the four major multilateral treaties on cybercrime in force,[10] the still-relatively limited coverage of existing multilateral treaties led the Twelfth UN Congress on Crime Prevention and Criminal Justice in 2010 to conclude that serious consideration ought to be given to developing a further convention to combat cybercrime.[11] That call prompted a discussion on **(F)** what lessons have been learned that could enhance membership in formal international instruments. For State Parties, binding multilateral instruments on cybercrime, as well as other more general anti-crime instruments with international cooperation provisions that can be used to combat cybercrime, provide the basic normative framework for addressing cybercrime.

While treaties are, by and large, a positive, their proliferation can be of an issue. One underlying purpose of a treaty is to encourage cooperation among its Member States or Contracting Parties on the subject matter of the treaty. However, the growing number of treaties and international agreements regarding cyberspace poses challenges to ensuring interoperability of the various instruments, as well as effective cooperation among countries that may be members of different instruments and may have different obligations regarding cooperation, especially regarding MLA (discussed below). A more in-depth comparison of the contents of the various cybercrime treaties can be found in appendix 9 B.

A. Budapest Convention

The Budapest Convention of 2001 is the foremost international instrument on cybercrime, in part because it is the only truly "global" instrument, being open to signature by non-CoE Member

States.[12] A great deal of great value has already been written about the Budapest Convention; through a few observations are warranted, the Toolkit does not attempt to either repeat or summarize those commentaries.

The Budapest Convention combines a comprehensive set of rules on different aspects of cybercrime including substantive, procedural, jurisdictional and international cooperation issues.[13] The Convention is legally binding on its Member States. Its clear definition of criminal offenses as balanced against procedural safeguards[14] is an excellent example of good practice. In addition, it contains important provisions requiring Contracting Parties to observe due process and human rights while combatting cybercrime.[15] While accession is not limited by geography, accession of non-CoE Member States is restricted to those "invited" upon the unanimous consent of the Contracting Parties to the Convention[16]; understandably, eighty-four percent of the Convention's signatories are CoE Member States.[17] Saying that, the Convention was developed with the participation of four states that are not CoE Member States,[18] and another seventeen non-Member States have either acceded to the Convention or have been invited to do so.[19]

B. Commonwealth of Independent States Agreement

The CIS Agreement of 2001[20] seeks to encourage cooperation in assuring the effective prevention, detection, suppression, uncovering and investigation of cybercrime offences. To do so, Parties agree to adopt such organizational and legislative measures as may be necessary to implement the provisions of this Agreement, and to strive to ensure the harmonization of their national legislation concerning the combating of offences relating to computer information. While, as with the Budapest Convention[21] and the SCO Agreement (discussed below),[22] accession is not limited by geography, accession is contingent upon the agreement of all Parties.[23] Unlike the Budapest Convention, however, the CIS Agreement was developed by all of its twelve Member States[24]; thus, it is unsurprising that only CIS Member States have acceded. However, while all twelve CIS Member States signed, only six have ratified,[25] with one other state (Russia) having sent notification in 2004 that internal procedures for ratification are underway.[26]

C. Shanghai Cooperation Organization Agreement

With the SCO Agreement of 2009,[27] the heads of government of the six SCO Member States reaffirmed that current science and technology conditions warranted cooperation in order to enhance the capability of SCO Member States to confront global challenges and threats.[28] Like the Budapest Convention[29] and the CIS Agreement,[30] accession to the SCO Agreement is not limited by geography.[31] All six SCO Members States have signed the Agreement.[32]

D. League of Arab States Convention on Combating Information Technology Offences

The Arab Convention.[33] The Arab Convention adopts a common criminal policy, which serves to enhance and strengthen cooperation in the area of combating information technology offenses that threaten security and interests of Member States and the safety of their communities with specific reference to the importance of Islamic law.[34] Parties agree to implement procedural and legislative policies, which both criminalize technology offences, and which facilitate the prosecution of cybercrimes, and the tracking and collection of digital evidence. There is noted deference to equality of the regional sovereignty of states and noninterference in the internal affairs of other states.[35] Unlike the Budapest Convention,[36] the SCO Agreement[37] or the CIS Agreement,[38] accession is contingent on membership to the League of Arab States.[39] Of the twenty-two member States (with Syria's membership having been indefinitely suspended), eighteen have signed.[40]

E. African Union Convention on Cyber Security and Personal Data Protection

The most recent of international instruments is the AU Convention of 2014.[41] Although the AU Convention is a positive step in the progress of the fight against cybercrime, and an undeniable statement of regional political expression, it diverges substantially from other instruments (both international and domestic); as such, that make the AU Convention is a less useful or desirable model upon which to build, notably in terms of safeguards (*see* sections 4 A and 4 B, above) and the binding legal nature of the AU Convention in the area of MLATs, for example.[42] Moreover, of the fifty-four AU Member States, only right have signed the AU Convention, and none have ratified it.[43] The AU Convention requires fifteen instruments of ratification in order to enter into force.[44]

F. Areas of Improvement for Formal International Agreements

Many of the formal international instruments combatting cybercrime have been in existence for up to fifteen years. In the age of the internet, this is, if not a lifetime, certainly a generation. The instruments have proved both flexible and encouraged signatories and non-signatories alike to take action to ensure greater interoperability of legal frameworks.[45] That said, while more and more countries from more and more places around the globe are adhering to cybercrime treaties, coverage is still far from universal. Furthermore, there are substantive divergences among those instruments.

Some areas for consideration in the next generation of international instruments follow:

- **Inclusion.** To attract interest—and ownership—from all states, space needs to be created to include them in the consideration of the instrument from an early stage.
- **Multi-stakeholdersim.** Stakeholders have grown and diversified. In particular, in recognition of the role that private sector actors increasingly play in the fight against cybercrime, effective ways of encouraging cooperation with law enforcement should be explicitly addressed.
- **Incorporating lessons learned.** Cybercrime is evolving. Cybercrime is evolving. Many of the existing instruments may need modification or renewal. There is an inherent tension in any instrument between being sufficiently flexible to accommodate evolving cybercrime, and being too vague or general; each dimension may require different types of adjustment.
- **Overcoming persistent limitations in coverage.** Perhaps related to inclusion, uptake of membership in international instruments, despite the openness of the Budapest Convention and the proliferation of regional and sub-regional instruments while growing, is still relatively low.
- **National implementation.** Joining any of the instruments is not in and of itself the ultimate goal; it is only the starting point. What is really required, ultimately, is national domestication of the terms of those instruments, and subsequent implementing and practicing those requirements by appropriate authorities.
- **International instruments aggravate differences among states.** Because of the variability of implementation of national laws to reflect treaty-based obligations (that is, differences in national laws), cooperation obligations in treaties may exacerbate different approaches. For example, rights of the accused may vary from country to country, but MLA provisions may require assistance, thus potentially facilitating abuses, especially in areas of dual criminality.
- **Safeguards.** Not all the instruments provide safeguards for protecting due process (*see* section 4 A, above) and other fundamental rights, notably in matters of privacy and/or data protection and of freedom of expression (*see* section 4 B, above).

II. Mutual Legal Assistance Treaties

This subsection first provides a **(A)** general overview of the nature and general aspects of MLATs, and then **(B)** examines how these aspects are treated in multilateral instruments using the example of the Budapest Convention's MLA provisions.

A. General Aspects of MLATs

MLATs are agreements between two or more countries for the purpose of gathering and exchanging information in order to enforce public or criminal laws. While binding multilateral instruments provide an important basis for international cooperation,[46] even non-binding MLATs

(which have been particularly influential in Caribbean and African countries) offer valuable guidance on international or regional standards for dealing with cybercrime.[47] Moreover, states having entered into MLATs tend to adopt domestic law on cybercrime.[48] In addition, there are a number of regional instruments dealing with MLA in the broader criminal context.[49]

According to UNODC, extra-territorial evidence in cybercrime cases is obtained through traditional forms of cooperation, with over seventy percent of reporting countries using formal MLA. Within such formal cooperation, almost sixty percent of requests use bilateral MLATs as the legal basis. Multilateral MLATs are used in twenty percent of cases. Response times for formal mechanisms were reported to be of the order of months, for both extradition and MLA requests, a timescale that presents particular in the cybercrime context, as electronic evidence is typically volatile by nature.[50] Initiatives for furthering informal cooperation and for facilitating existing formal cooperation, such as 24/7 networks, offer important potential for faster response times (*see* section 5 B, below).[51]

While MLATs can be formed at a multilateral or bilateral level, unfortunately, over sixty percent of countries are not party to any multilateral cybercrime instrument, meaning that they have no international legal obligation to either include specialized cybercrime investigative powers in national procedural laws, or to carry out specialized investigations in response to cooperation requests.[52] Indeed, UNODC has noted "modes of informal cooperation are possible for around two-thirds of reporting countries, although few countries have a policy for the use of such mechanisms."[53]

Box 5.1: Korea
Example of Legislation on International Judicial MA in Criminal Matters[54]

"**Art. 5:** The scope of mutual assistance shall be as follows: (1) Investigation into the whereabouts of a person or object; (2) Provision of documents and records; (3) Service of documents, etc.; (4) Gathering of evidence, seizure, search, and verification; (5) Transfer of objects, such as evidence; (6) Hearing of statements, and other measures to make any person testify or cooperate with an investigation in the requesting country.

"**Art. 6:** Mutual assistance may not be provided in any of the following cases: (1) Where it might be detrimental to the sovereignty, national security, public peace and order, or public morals, of the Republic of Korea; (2) Where it is deemed that the criminal might be punished, or subject to an unfavorable penalty disposition, due to his/her race, nationality, gender, religion, social status, or the fact that he/she is a member of a specified social organization, or by the reason that he/she has a different political view; (3) Where it is deemed that the crime under mutual assistance is of a political nature, or a request for mutual assistance is made for the purpose of an investigation or trial on another crime of a political nature; (4) Where the crime under mutual assistance does not constitute a crime, or it is a crime against which

no public action may be instituted, under any Act of the Republic of Korea; (5) Where the requesting country fails to give a guarantee although this Act prescribes that the requesting country should do so."

With mechanisms for requesting and obtaining evidence for criminal investigations and prosecutions, MLATs remain one of the most comprehensive tools for building an interoperable legal framework at the international level, and, therefore, for overcoming jurisdictional issues. MLATs allow signatories to shift from strict territorial views to more comprehensive and cooperative views,[55] providing them with reciprocal abilities to obtain jurisdictional power over offenses (*see* section 2 E, above).

MLATs, though effective tools, are far from perfect. Frequently, they are not particularly extensive, and, in order for them to have effect, signatories typically must first introduce and domesticate the treaty's provisions into their own legal systems through legislation or other appropriate means.[56] Moreover, it is commonly lamented that MLAT facilitation mechanisms are difficult and take time to effectuate.[57] While efforts are underway globally to improve these processes, many factors combine to impede progress. Such hindrances are of particularly great concern in combatting cybercrime, where evidence is often fragile and fleeting, and where it is found in a world—cyberspace—where identity and anonymity are easily created and recreated. Similarly, as the location of the perpetrator may be difficult to identify, determining which entities have control over the desired data may be complicated. Indeed, even once the perpetrator's location has been identified, the desired data may not be so easy to identify and locate, a matter complicated both by the facile manner in which data might be moved, and by technology developments, such as cloud computing, that allow the fragmenting and (re)routing of data through several countries (*see* section 2 C, above).

All of the above elements together frequently make it unclear which state has legal jurisdiction over the data. As a result, an increasing number of states are asserting jurisdiction to continue electronic investigations even when, in the physical world, that action might be considered an infringement of another state's sovereignty. For instance, antitrust investigators of Belgium, Brazil, and the EU, among others, assert the right to conduct electronic searches in certain circumstances, even where they are aware that the search will take place outside of the physical territory in which they have authority and know to which country an MLA request could be sent. While these assertions of investigative jurisdiction may be proper under the law of the states or organizations that undertaking such actions, they may be considered as improper by the states where the data is located, or by the investigated party. As such, some states disallow such searches entirely, creating further obstacles to interoperability.

As the principle challenge to MLA requests is typically lenghty response times,[58] three of the major multilateral treaties on cybercrime—the Budapest Convention,[59] the CIS Agreement[60] and the Arab Convention[61]—seek to expedite matters by requiring Member States to designate points-of-contact for MLA requests. Relatedly, in order to facilitate the gathering of electronic evidence,

the same three instruments provide rules on expedited means of communication or other urgent channels for MLA requests.[62] However, as these treaties are only binding on their Member States, non-Member States are less likely to have such urgent (or clear) channels for MLA requests in place in comparison to Member States of those treaties.[63]

B. Budapest Convention's MLA Provisions

The Budapest Convention is the most extensive MLAT on cybercrime. Designed with the purpose of fostering cooperation on cybercrime,[64] the Convention comprehensively covers those actions that Parties are to criminalize in their domestic law as cybercrimes (*see* section 2 B, above), before going on to address procedural and evidentiary issues. The Convention stipulates that each Party is to implement laws giving it jurisdiction over offenses committed: (1) within its territory; (2) on board a ship flying its flag; (3) on board an aircraft registered under its laws; or (4) by one of its nationals.[65] In so doing, the Convention combines the principle of territorialty with that of active nationality. It does not, however, utilize other available principles for extending jurisdiction (*see* section 2 E, above). That said, the Convention does not exclude Parties from unilaterally using such principles to expand jurisdictional requirements.[66]

In addition to obliging Parties to criminalize the offenses that it enumerates, the Budapest Convention also obliges Parties to ensure that that procedural tools are available to investigate the enumerated crimes, as well as other crimes not listed in the Convention.[67] Doing so is a recognition of the importance of electronic investigations in any type of crime, and at any stage of development. For instance, mobile-phone data may be indispensable to combatting human trafficking, corruption, narcotics or child exploitation. The Convention's procedural tools are tailored to avoid violations of sovereignty and human rights, while still enabling states to adequately investigate crimes.[68]

Of particular note is the matter of expediency. The Convention makes significant strides towards improving the timeliness with which cybercriminal matters are addressed between Parties. One such mechanism is had by requiring each state to create a "24/7 Network",[69] a matter that, though introduced through formal means, sets up substantial opportunities for developing the often-more effective methods of informal cooperation (*see* section 5 B, below).

III. Extradition Treaties

This subsection discusses **(A)** the general nature and aspects of extradition treaties, and then **(B)** uses the provisions of the Budapest Convention as an example.

A. General Aspects of Extradition Treaties

While MLATs focus on the cross-jurisdictional gathering and exchanging of information, extradition treaties aim to create a means for giving jurisdiction over the perpetrator—what is frequently called physical or personal jurisdiction—to the state desiring to prosecute (referred as the "requesting state"). Extradition treaties are the most common form of international cooperation for obtaining jurisdiction over the alleged perpetrator, who is often referred to as the "target". Although extradition is frequently included as an element in MLATs,[70] separate, standalone agreements are often agreed upon. The core provisions of an extradition agreement create assurances and procedures for the custodial state to honor a warrant issued by the requesting state, thereby obliging the custodial state to take the target into custody and arrange transfer to the requesting state.[71]

Extradition treaties operate under the principle of *aut dedere aut judicare*—"extradite or prosecute".[72] However, and notwithstanding that guiding principle, extradition agreements are often limited by crime type,[73] and have carve-outs and disallowances—for instance, the European Convention on Extradition disallows extradition where the offense for which extradition is sought is considered political in nature, or where it is punishable by death under the law of the requesting state.[74] In instances where the target is a national of the custodial state, or where the custodial state has created some other legal basis necessary for prosecuting the target, that state may prosecute and punish before extraditing to the requesting state.[75]

Where cybercrime is concerned, the effectiveness of extradition treaties may be hindered by the requirement of what is called "dual criminality". Dual criminality is the concept that extradition can only be allowed if the allegedly illegal act is a crime in both states.[76] For instance, in the case of the "Love Bug" virus, the absence of legislation criminalizing computer crimes in the custodial state (in this case, the Philippines) not only precluded local prosecution of the believed-Filipino hacker, but also prevented foreign authorities (notably, the FBI) from seeking extradition under the applicable agreement due to the requirement of dual criminality (*see* section 2 E, box 2.7, above).

B. Budapest Convention's Extradition Provisions

The Budapest Convention includes specific provisions for extraditing a target.[77] However, the obligation to extradite is limited, first, to offenses established in accordance with the Convention, second, by the principle of dual criminality, and, third, to offenses that are punishable by the deprivation of liberty for a maximum period of at least one year or by a more severe penalty.[78] This last element—the threshold penalty—was introduced because it was not considered appropriate to require that each of the offences be considered *per se* extraditable, as Parties might, in their own sovereign discretion, prescript different incarceration periods.[79] It bears noting that the determination of whether an offender is extraditable hinges upon the maximum period that may legally be imposed for a violation, not upon the actual penalty imposed.[80] Moreover, the

Convention allows for coupling with other extradition treaties: where another extradition treaty exists, the offenses of the Budapest Convention might be deemed extraditable offences under that other treaty,[81] thereby potentially expediting matters, especially with states not party to the Convention.

Conclusion

The inherently transnational, cross-border nature of cybercrime has led to jurisdictional issues—over the crime, the evidence and the alleged perpetrators—that require international cooperation if they are to be overcome. The most effective and efficient means of doing so is through formal instruments, as supplemented through informal mechanisms. There is a threefold lack that these formal instruments attempt to overcome, namely: lack of criminal laws, lack of procedural powers and lack of enforceable MLA provisions.[82] The three major means for filling-in these gaps comes through cyber-specific multilateral MLATs, more general MLATs and extradition treaties.

The most comprehensive and influential cyber-specific instrument is the Budapest Convention. A leading example of how to address the most urgent issues in the domain of cybercrime, its binding nature on Parties has increased its efficacy and suits its aspirational goal of harmonization—an ambition somewhat beyond interoperability—in this area. Moreover, the indirect impact of the Convention has unquestionably been far-reaching, serving as a model for legislation, offering general guidance and sparking substantial debate the world over. The Convention has done much to further international cooperation, even among states that already enjoyed good relations.[83]

Notwithstanding its limitations, the Budapest Convention has many strengths, leading one commentator to say that:

> "[I]t is likely to remain the most significant international legal instrument in the field for the foreseeable future."[84]

B. Establishing Informal International Cooperation

Table of Contents

Introduction

This chapter begins, and much of the Toolkit has discusses, the place of formal, international agreements, it does so on the understanding that sovereignty resides with states; however, it does so while keeping an eye to finding global consensus and to promoting international interoperability. However, and for various reasons, formal mechanisms of international cooperation have generally only sketched out the larger cooperative space, leaving a great deal for states to fill in through informal and ad hoc cooperation.

As the division between the formal and the informal is often subtle, the Toolkit uses the more clearly delineated provisions of international instruments as indicative of formal mechanisms of international cooperation, leaving the unspoken spaces where

cooperative acts have occurred to the realm of informal cooperation. Notwithstanding that distinction, this section begins by **(I)** acknowledging that calls for informal cooperation often come from international sources, a reality that deserves discussion in order to better understand and contextualize the environment in which informal international cooperation is situated. In considering informal mechanisms of international cooperation, particular note should be paid to **(II)** 24/7 networks and **(III)** information sharing and coordination centers, the skeleton of which formal instruments have laid out, but the meat of which is largely left to states to put on as they see fit. Somewhat separately, it should be recalled that **(IV)** inter-institutional collaboration can achieve important results. Less visible but also important are **(V)** efforts to improve interoperability by standardizing information requests and authentication procedures.

I. The Place for Informal Cooperation

Governments, international organizations and non-governmental organizations alike have all proposed various options supporting international interoperability. For example, in 1990 the UN General Assembly adopted a resolution dealing with computer crime legislation.[1] In 1997, the G8 released a Ministers' Communiqué that included an action plan and principles for combatting cybercrime and protecting data and systems from unauthorized impairment.[2] In 2003, the World Summit on the Information Society (WSIS) issued the Geneva Declaration of Principles and Plan of Action, which highlighted the importance of cooperative measures in building confidence and security in the use of ICTs.[3]

As discussed,[4] formal measures, notably the Budapest Convention, the Council of Europe's 2001 contribution to the quest for international interoperability, help lay a shared framework upon which other informal efforts might be laid. European efforts have particularly focused on overcoming procedural obstacles that pertain to the principles of territoriality and of national sovereignty, and that hamper international computer crime investigations.[5] While the highly visible Budapest Convention may largely set the structure,[6] much of the work is done through a number of general EU-instituted[7] measures to facilitate police cooperation at the operational level.[8]

II. 24/7 Networks

With borders serving as no hindrance to cybercriminals, and with time zones often helping to

cloak their illegal activities from immediate notice, effectively combatting cybercrime requires an internationally-tasked, constantly-active response network that integrates national law enforcement agencies. Because "crime never sleeps", individual countries should designate directly reachable point-persons for every hour of every day, with contact information kept current. In order for 24/7 networks to operate effectively, national point-persons must understand their own legal and policy framework; how their domestic arrangements intersect and interact with the larger international systems function; have the minimum technical knowledge to understand cybercriminal behavior; and must be capable of communicating in foreign languages, with English language skills being a minimum.[9]

Several authorities have created such a network, three of which are of particular note: **(A)** the G8,[10] **(B)** the Budapest Convention and **(C)** INTERPOL.

Table 5.1: Various 24/7 Networks

Network Name	Date	Members	Organizing Authority
G8 24/7 Network for High-Tech Crime	Jun. 2015	70	G8 High-Tech Crime Subgroup
Budapest Cybercrime 24/7 Network	Sep. 2015	55	CoE
INTERPOL Global Police Communications System	Jun. 2015	136	INTERPOL

A. G8 24/7 Network for Data Preservation

Through its Lyon-Roma[11] High Tech Crime Subgroup (HTCSG),[12] the G8 proposed its 24/7 Network for Data Preservation.[13] Becoming operative in 1999,[14] and gaining further impetus from the G8 Deauville summit in 2011,[15] the network has seventy members today. Its focus is on creating cyber-specialized points-of-contact for incidences requiring urgent assistance with investigations involving electronic evidence. The Computer Crime and Intellectual Property Section (CCIPS) of the US DoJ manages new memberships for the HTCSG and is responsible for periodic updates of information on the point-of-contacts. Further efforts to develop a training initiative will further develop not only the necessary cybersecurity capacity-building, but also boost international understanding and cooperation.[16] An example of informal international cooperation facilitated through international instruments, such trainings are not only a vital part in the fight against cybercrime, but also an example of the propulsive effect that international agreements and instruments—even if not formalized at the level of a treaty—can have.

B. Budapest Convention 24/7 High Tech Crime Points of Contact Network

The Budapest Convention requires Parties to create a 24/7 High Tech Crime Points of Contact Network.[17] Parties are required to "designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence."[18] That assistance is intended to facilitate the provision of technical assistance, data preservation, evidence collection, legal aid and assistance locating suspects.[19] The Convention goes so far as to permit those measures to be directly carried out by the requesting state, its domestic law and practice allowing.[20] The 24/7 Network has proven quite effective, with its "services [proving…] invaluable in helping to ensure that investigators could preserve and seek the information they needed to investigate the emergency".[21]

C. INTERPOL I-24/7 Global Police Communications System

INTERPOL's I-24/7 Global Police—which it calls the "foundation of information exchange between the world's police"—is a worldwide communications system connecting law enforcement officers in INTERPOL Member States.[22] Through each state's domestically-staffed National Central Bureau (NCB), authorized users—typically frontline law enforcement officers—can share sensitive and urgent police information with their counterparts around the globe on a 24-hour-a-day, 365-day-a-year basis with direct access to INTERPOL's range of criminal databases, including databases on suspected criminals or wanted persons, stolen and lost travel documents, stolen motor vehicles, fingerprints, DNA profiles, stolen administrative documents and stolen works of art.[23] Preparations are underway to extend access to INTERPOL services beyond the NCB to additional frontline officers, including immigration and customs officials.[24] In order to further expedite assistance, each state's NCB designates a National Central Reference Point for Computer-Related Crime (NCRP), who is available through an INTERPOL-managed hotline. Among other things, it features an early warning system between cybercrime investigation units.

Box 5.2: Korea Activates 24/7 Network to Secure e-Evidence

On 23 December 2014, cybercriminals successfully hacked the computer systems of South Korea's state-run nuclear operator, Korea Hydro and Nuclear Power Co. Ltd. (KHNP).[25] KHNP, which operates Korea's twenty-three large reactors and its many hydroelectric plants, is responsible for about forty percent of the country's electric power supply.[26] Although there was no evidence that the nuclear controls systems were hacked, sensitive information, including blueprints of nuclear plant equipment, electricity flow charts and estimates of

radiation exposure among local residents, was stolen, some of which was posted on the internet via Twitter.[27] The hackers demanded that three of the reactors be shut down, as well as an unspecified amount of money, threatening, in a message posted on Twitter, to "bring destruction" to the power plants if the demands were not met.[28]

Utilizing the G8 24/7 Network, the Korean point-of-contact sent email and telephone requests to the US point-of-contact asking that digital evidence in the relevant Social Networking Service (SNS) accounts to be preserved. The US point-of-contact subsequently turned to the ISPs managing the relevant accounts, activating protocols enabling the disclosure of evidence in emergency situations. Within twenty-four hours after the request, information on the offenders' SNS accounts and access logs had been delivered to the Korean investigative team.

III. Information Sharing & Coordination Centers

While cooperative 24/7 networks can help preserve digital evidence located in other jurisdictions,[29] law enforcement has repeatedly lamented the absence of mechanisms to enter electronic networks and to expeditiously preserve computer data, such as connection logs.[30] Due to cybercrime's inherently transnational and cross-jurisdictional nature, at any moment, and from any part of the world, cybercriminals can attack multiple targets. As such, leaving a country's law enforcement to independently conduct investigations could end up with only partial findings. Moreover, operating independently might inadvertently—and inopportunely—influence investigations in other countries, for instance, by alerting targets, disclosing information, or destroying evidence. Furthermore, the deterrent effect is limited where only certain members of multinational crimes are prosecuted; such is especially true in instances where a state lacks the capacity or resources to investigate and prosecute, thereby encouraging cybercriminals to act with impunity.

Several global information sharing and coordination centers have emerged, notably **(A)** INTERPOL's Global Complex for Innovation, **(B)** Europol's European Cybercrime Center, **(C)** the EU's Judicial Cooperation Unit, **(D)** the US National Cyber-Forensics and Training Alliance, **(E)** the Commonwealth Cybercrime Initiative and **(F)** OAS initiatives.

A. INTERPOL's Global Complex for Innovation

Recognizing that technological developments mean police worldwide face an increasingly challenging operational and cross-global landscape, the INTERPOL Global Complex for Innovation (IGCI) opened in Singapore in June 2015.[31] A cutting-edge research and development facility for the identifying of crimes and criminals, providing innovative training, offering operational support and nurturing partnerships, IGCI places an emphasis on developing and enhancing open-source

forensics cyber tools for local law enforcement. Recent technical innovations have transformed the nature of crime fighting, and open-source forensics tools are particularly favorable as they are so useful for police departments in poor and developing nations. In addition to improving formal, national capacity-building by encouraging and supporting domestic development, IGCI also supports informal cooperation by stationing police officials from various countries at its headquarters. As such, IGCI not only furthers both information sharing but also the larger object of inter-governmental coordination. IGCI is the product of the recognition that combatting cybercrime requires interoperability in both formal and informal ways.

Effectively, IGCI is a space for law enforcement to learn about the latest cybercrimes, and to have their work supported by state-of-the-art digital forensics laboratories and research stations. Moreover, as real-time access to criminal data is crucial in today's technologically innovative and rapidly changing world, private sector and academia, IGCI also serves as an important means for building innovative public-private partnerships by integrating the private sector and academia into its activities. The digital forensic laboratory conducts analysis of criminal trends, tests forensic devices, develops good practices and supports empowerment training. The cyber fusion center analyzes information from the private sector and academia, which it provides to Member States in support of their investigations.

The placement of IGCI in Asia was not merely a piece of savvy politicking[32] but a conscientious decision: by working in coordination with INTERPOL's General Secretariat, seated in Lyon, France[33] and its recently established Command and Coordination Centre (CCC) in Buenos Aires, Argentina[34] constant, global coverage is guaranteed.[35] This strategic geographic placement facilitates the combatting of cybercrimes that have targets, not only in multiple jurisdictions, but also in multiple and differing time zones, and which often take place using co-conspirators located in various countries, using ICT systems sitting in equally divergent countries.

B. Europol's European Cybercrime Center

Another model for information sharing and coordination is Europol's European Cybercrime Center (EC3).[36] Set up in January 2013, EC3 is tasked with following cybercrimes committed by organized groups (especially, for instance, online fraud); that cause serious harm to the victim (*e.g.*, online child sexual exploitation); and that affect critical EU infrastructure and information systems (*e.g.*, cyberattacks).[37] As with the IGCI, EC3 collects criminal information, supports investigation, assists in digital forensics, pursues research and development provides and education and training.

Strategically situated within Europol both to draw on Europol's existing law enforcement capacity and to expand Europol's existing capabilities, EC3 serves as the central EU hub for criminal information and intelligence, while also supporting Member States' operations, providing strategic analysis products and providing highly specialized technical and digital forensic support capabilities.[38] Staffed by cyber liaisons officers and analysts seconded from EU Member States, as well as from certain non-Member States, EC3 also supports training and capacity-building, and

serves as a comprehensive outreach function connecting cybercrime-related law enforcement authorities with the private sector, academia and other non-law enforcement partners.[39]

The value of coordination and cooperation has been recognized, leading to the creation of the Joint Cybercrime Action Taskforce (J-CAT). Launched in September 2014 as a six-month project to facilitate joint investigations, the Taskforce has the objective of proactively driving intelligence-led, coordinated action against key cyberthreats and top targets.[40] J-CAT is specifically involved with high-tech crimes (such as malware, botnets and intrusion), crime facilitation (such as bulletproof hosting, counter-anti-virus services, infrastructure leasing and rental, money laundering, including virtual currencies), online fraud (online payment systems, carding, social engineering) and the various aspects of child sexual exploitation online.[41]

C. EU's Judicial Cooperation Unit

Police-to-police efforts are not the only forms of international information sharing and operational coordination. The EU's Judicial Cooperation Unit (Eurojust) is an example of international judicial coordination. Set up in February 2002 (but with its origins going back to 1999),[42] it is composed of national prosecutors, magistrates and police officers of equivalent competence that are detached from each Member State according to their own legal system. Its mission, enshrined at the heart of the European Union by the Treaty of Lisbon, is "to support and strengthen coordination and cooperation between national investigating and prosecuting authorities in relation to serious crime affecting two or more Member States [….]"[43] In particular, it assists by facilitating the execution of MLATs and extradition treaties.[44] Eurojust has been central to negotiating cooperation agreements with third states and among EU agencies, allowing the exchange of judicial information and personal data.[45]

Eurojust maintains a network of contact points worldwide that serve as "active intermediaries", including the twenty-eight EU Member States, as well as contact points in twenty-three non-Member States.[46] It also has privileged relationships with the European Judicial Network (EJN), Europol, the European Anti-Fraud Office (OLAF) and Liaison Magistrates.[47] In this discussion, the relationship with EJN, which is composed of more than three hundred national contact points throughout the EU Member States, is of particular note.[48] Although not an EU entity, it bears noting that the Global Prosecutors E-crime Network (GPEN) of the International Association of Prosecutors (IAP)[49] provides networks of national contact points for the facilitation of judicial cooperation, with which Eurojust frequently communicates. These networks focus on personnel exchanges designated by nations and interchanges of expertise by organizing regular conferences and meetings, as well as publishing relevant materials.

Now permanently seated in The Hague alongside Europol,[50] Eurojust's competence covers the same types of crime and offences for which Europol has competence, including terrorism, drug trafficking, trafficking in human beings, counterfeiting, money laundering, computer crime, crime against property or public goods including fraud and corruption, criminal offences affecting

the European Union's financial interests, environmental crime and participation in a criminal organization.[51] For matters beyond those for which it has competence, Eurojust may be called to assist in investigations and prosecutions at the request of a Member State.[52] Eurojust serves as an organizational and orchestrating authority for cross-Member State matters, with power to ask the competent authorities of concerned Member States concerned to investigate or prosecute specific acts, to coordinate with one another, to determine that one state is better placed to prosecute than another, to set up a Joint Investigation Team, and to provide Eurojust with information necessary to carry out its tasks.[53]

In December 2008, Ministers of Member States at the Justice and Home Affairs Council adopted a revised Council Decision on the strengthening of Eurojust, notably by increasing information interchange, and by making Eurojust available to national authorities on a 24/7 basis.[54]

Box 5.3: Operation BlackShades

BlackShades was an organization developing and selling malware that enabled buyers to infect and take control of computers—for instance, one buyer infected at least 2,000 computers, controlling the victims' webcams to take pictures of women and girls.[55] A US FBI investigation revealed links to several EU Member States,[56] certain of which had already begun their own independent investigations.[57] Sellers and users of BlackShades malware were targeted by judicial and law enforcement authorities in sixteen states during this worldwide investigation.[58]

Eurojust, supported by EC3, subsequently coordinated a common operation. Beginning in November 2013 with information sharing and the coordinating of actions, the operation culminated in May 2014 with a two-day strike involving actions in sixteen countries (the Netherlands, Belgium, France, Germany, the United Kingdom, Finland, Austria, Estonia, Denmark, Italy, Croatia, the United States, Canada, Chile, Switzerland and Moldova).[59] Over those two days, 359 house searches were carried out worldwide, 97 people arrested and over 1,100 data storage devices suspected of being used in the illegal activities were seized.[60] Substantial quantities of cash, illegal firearms and drugs were also seized, as was the domain of the BlackShades website.[61] Eurojust assisted the involved states by delivering overviews of the status of the investigations in each state and by providing judicial assistance, with EC3 providing real-time analytical support. Eurojust also played a key role in determining the optimal country for prosecution.

D. US National Cyber-forensics & Training Alliance

The National Cyber-Forensics & Training Alliance (NCFTA)[62] was established in 2002 as a non-

profit corporation focused on identifying, mitigating and ultimately neutralizing cyberthreats through strategic alliances and partnerships with Subject Matter Experts in the public, private and academic sectors.[63] Jointly founded by the FBI, the investigative branch of the DoJ,[64] and InfraGard, a partnership between the FBI and the private sector that operates as an association of persons representing businesses, academic institutions, state and local law enforcement agencies and other participants dedicated to sharing information and intelligence to prevent hostile acts against the United States.[65] Headquartered in Pittsburgh, Pennsylvania, the NCFTA has offices in Los Angeles, California and New York, New York[66] and has strategic partnerships with institutions around the world.[67] The NCFTA shares information on emerging cyberthreats and resources, including Subject Matter Experts, on a real-time basis across all sectors and with all partners via multiple communication channels.[68] Foreign cyber law enforcement officers are embedded at NCFTA for extended periods.

The most valuable and effective means of communications of NCFTA network is verbal, face-to-face communication that happens daily, in the neutral environment of trust that NCFTA has built. Such efforts are proactive and preventative, thereby enabling NCFTA to give early warnings relating to cyberthreats and cyber transactions, as well as to assist partners in protecting their brand, reputation, shareholder value, economic losses and customer confidence.

In an effort to streamline intelligence exchange, NCFTA regularly organizes interaction into threat-specific initiatives. Once a significant cybercrime trend is realized and a stakeholder consensus defined, an initiative is developed wherein NCFTA manages the collection and sharing of intelligence with industry partners, appropriate law enforcement and other cross-sector SMEs. Each initiative analyzes real-time resources to identify threats, threat actors and provide actionable intelligence to industry and law enforcement to neutralize the threats. Through NCFTA initiatives, hundreds of criminal (and some civil) investigations have been launched which would not otherwise have been addressed. Currently, NCFTA has aided in successful prosecutions of more than three hundred cyber criminals worldwide. Furthermore, NCFTA has produced more than eight hundred cyberthreat intelligence reports over the past three years alone to support these initiatives.

Law enforcement and private sector entities are co-located at NCFTA.[69] In this regard, if, for example, a private sector entity, such as a bank or credit card company, is a victim of a cyberattack, then that entity can immediately pass any relevant information on to other NCFTA members. With the support of law-enforcement agency representatives who are also located at NCFTA headquarters, members can then use that information to open or advance existing investigations in concert with global partners. NCFTA supports specialized and targeted programs, including the Cyber Financial Program (CyFin), which is dedicated to the identification, mitigation and neutralization of cyberthreats to the financial services industry[70]; the Brand and Consumer Protection (BCP) Program, which focuses on keeping the internet as a safe place for the sale of retail goods[71]; and the Malware and Cyber Threats (MCT) Program, which researches, identifies and provides timely alerts through data feeds and proactive intelligence on cyberthreats under analysis.[72]

The success of NCFTA is in large measure due to the relationships it has engendered between the public and private sectors. Indeed, collaboration and cooperation among private industry, academia and law enforcement has been critical to their continued success and effectiveness.[73]

E. Commonwealth Cybercrime Initiative

The Commonwealth Cybercrime Initiative (CCI)[74] is a capacity-building program of the Commonwealth Secretariat aiming to assist member states through multi-stakeholder partnership providing coherent, comprehensive and sustainable assistance to reduce cybercrime.[75] Bringing together forty international organizations—including INTERPOL, OAS, CoE, the Commonwealth Telecommunications Organisation (CTO) and ITU—to form the CCI Consortium, it helps put on multidisciplinary programs in Commonwealth countries.[76] It brings additional resources to the Commonwealth Model Law on Cybercrime and to the Harare Scheme for MLA.[77] The CCI deserves notable attention for, while it and both the Model Legislation and the Harare Scheme are voluntary and non-binding,[78] Commonwealth Heads of Government have given it an unambiguous mandate,[79] thereby providing CCI with unique political buy-in.[80]

The Commonwealth Secretariat is the focal point for CCI, with a representative from its Rule of Law Division sitting on CCI's Executive Management Committee[81] and providing secretariat.[82] CCI operates by deploying a mission team upon a member state's request. As an example of the good practices discussed above (*see* sections 2 C and 2 D, above) is that teams include both at least one technical and one criminal justice expert.[83] The team, which is drawn from CCI Consortium Member States best placed to donate the requisite resources, conducts a gap analysis based on the CCI Checklist,[84] from which a needs assessment report is produced.[85] The report's outcomes, which are agreed upon with the Member State, outlines priorities and capacities for reform, which the Consortium will then seek to develop. The program regional in its approach, has been active in both the Caribbean (*e.g.*, Trinidad and Tobago) and Africa (*e.g.*, Ghana, Botswana, Kenya, Uganda and Tanzania). Notable regional approaches to tackling cybercrime in which CCI has been central include the EAC Justice Network on Cybercrime and Electronic Evidence (in collaboration with UNODC)[86] and a still-nascent Caribbean organization.[87]

F. OAS Initiatives

Bringing together all thirty-five independent states of the Americas, the OAS constitutes the main political, juridical and social governmental forum in the Western Hemisphere, as well as the oldest regional organization in the world (dating to the First International Conference of American States, held in Washington, DC, from October 1889 to April 1890).[88]

OAS addresses cybercrime through two different projects. First, its Inter-American Committee against Terrorism has a launched the Cyber Security Program.[89] Tackling cybersecurity more broadly, and within the context of cyberterrorism,[90] it has established CIRTs in each country to

create a Hemispheric watch and warning network providing guidance and support, to cultivate and support NCSs (*see* section 2 F, above), and to promote a culture and awareness of cybersecurity.[91] While cybercrime is an element of that overall approach, it is relatively small one, with emphasis being placed on legislative criminalization and the implementation of appropriate legal tools.[92] Second, as part of the 1997 *Reunión Extraordinaria de los Ministros de Justicia de las Americas,* OAS set up, under the auspices of the Department of Legal Cooperation, both the Inter-American Cooperation Portal on Cyber-Crime and the Working Group on Cyber-Crime, which together aim at strengthening hemispheric cooperation in the investigation and prosecution of cybercrimes.[93] Among other things, this project has resulted in the creation of directory of national points of contact, cybercrime questionnaires and training for building capacity for combatting cybercrime.[94]

IV. Inter-institutional Collaboration

Informal international cooperation can also be had at the inter-institutional level. One example of inter-institutional collaboration can be seen in the East African Networking Meeting on Cybercrime and Electronic Evidence was held in Nairobi, Kenya from 19 to 20 August 2015. Organized by UNODC and COMSEC under the auspices of CCI (discussed above), the event was an important cooperative moment for both states and international organizations. The meeting's objective was to bring together criminal justice officials and key stakeholders from Member States of the EAC and other African states, as well as representatives of relevant intergovernmental and other organizations, to discuss and exchange information on national practices in, and experiences with, the prevention, investigation and prosecution of cybercrime.

The meeting devoted its main focus to the establishment of the East African Criminal Justice Network on Cybercrime and Electronic Evidence. The objectives were kept in line with the relevant action points set forth in the "Kampala Outcomes on Strengthening Regional Cooperation", as agreed at the EAC Regional Meeting on Preventing and Combating Cybercrime, held in Kampala, Uganda, in May 2014. The participants discussed a range of procedural and substantive aspects for the launching and operationalization of such a network, including its membership, chairmanship and functions, as well as its objectives and *modus operandi*. The network is to aim at (1) promoting the exchange of information and evidence between criminal justice and law enforcement counterparts; (2) facilitating working relationships between the criminal justice and law enforcement sectors and other key stakeholders; and (3) assisting formal and informal cooperation. As a result of the meeting, the participants agreed on the final text of the terms of reference of the network.

V. Standardizing Requesting Procedures

As a whole, improving interoperability on a procedural level requires at least as great a degree of understanding as it does on a substantive level. In addition to developing sufficiently robust

laws that allow for domestic authorities to conduct cybercrime investigations (*see* sections 2 C and 2 D, above), it is important for legislative measures to allow for foreign electronic evidence to be admissible in legal proceedings, as long as such evidence is gathered in a way of satisfying procedural legality. While legislative action will be required, it can be facilitated through informal arrangements, such as bilateral agreements, but also through the standardization of requesting procedures.

Developing standardized procedures for making information requests and authentication would greatly advance international interoperability.[95] While such would be especially the case once formal international instruments and systems have been put in place (*see* section 5 A, above), those arrangements might also be reached on a more informal level. Such procedures and understandings operate by building upon principles such as the flag principle, by which jurisdiction is somewhat more malleably understood (*see* section 2 E, above).

Control and possession of data has become an increasingly sensitive issue. For instance, the EU-US Safe Harbor Framework on transatlantic data flows was invalidated by the CJEU on the grounds that the scheme "enables [... US] public authorities [to interfere] with the fundamental rights of persons".[96] The fanfare—even alarm[97]—with which the decision was received, testifies to the ever-increasing importance of data—for both commercial and investigatory purposes—; and the rapidity with which a new EU-US arrangement (the so-called "Privacy Shield") was crafted[98] and adopted[99] reinforces that notion (*see* sections 4 A, and 4 B, above). In that sense, even attempts by some states to mandate that data pertaining to its citizens be stored on domestic servers, or made otherwise made automatically accessible (so-called "data localization"), could be construed by some to facilitate domestic law enforcement agencies. Moves towards data localization, however, would likely also multiply information requests, pacing burdens on both sides Additionally, while challenges to managing cross-border jurisdiction might be mitigated by data localization, the cross-border nature of cybercrime all but ensures that there will be continued need for cross-border exchanges.

As with efforts to improve MLA (*see* section 5 A, above), efforts are underway globally to speed-up international electronic investigations, while ensuring that they do not violate human rights. However, just as with efforts to improve MLA, efforts to speed-yet-constrain, remote cross-border electronic investigation have not yielded a resolution. For many years, the Council of Europe has been active in researching and discussing the issue of cross-border evidence collection, in which there is opportunity for participation by states not having acceded to the Budapest Convention in these discussion.[100]

Conclusion

Cybercrime can only be effectively investigated and prosecuted when supported through international cooperation. Formal means of such cooperation include multilateral treaties on

cybercrime, the most prominent of which is the Budapest Convention, as well as general MLATs treaties and extradition treaties. These instruments facilitate and further international investigations and prosecutions. However, those international instruments can only have full effect insofar as parties develop adaptive legal national frameworks (*see* sections 2 A, 2 B, 2 C, 2 D, 2 E and 2 F, above). Indeed, the biggest obstacle to international prosecution of cybercrimes is the dual criminality requirement.

Formal instruments of international cooperation are insufficient and must be supplemented through informal mechanisms. While the bones that arrange for informal interactions are often laid out in formal agreements, such as the Budapest Convention's 24/7 Network, it is for the individual states to truly put the meat on that skeletal framework. The informal communication encouraged through most 24/7 networks might be used prior to making a formal request for assistance, or in seeking expedited measures, such as data preservation, a matter typically not conducive to the more plodding procedures of MLATs. Moreover, by making use of 24/7 networks, law enforcement officials become accustomed to working with their counterparts, therein facilitating and furthering cooperation and capacity.

Information-sharing centers are another important means of rendering substance to the often-barebones mechanisms of cooperation. Through such centers, crucial cybercrime research and development can be conducted, shared resources brought to bear to support less resource-rich countries (including digital forensics laboratories), capacity-building developed and closer relations through personnel exchange had. Collectively, centers such as those created by INTERPOL (in Lyon, France, in Buenos Aires, Argentina and in Singapore) allow for global coverage at all hours of the day and night. Moreover, and no less importantly, such collaborations need not only be police-to-police, as the judicial collaborations of Eurojust and EC3 have effectively proven. Further, it bears noting that, in a world where real-time information is often crucial, finding analogues and partnerships for involving the private sector will be no less important to combatting cybercrime. Lastly, stardardizing requesting procedures could serve to significantly further formal international cooperation and interoperability.

End Notes

Referenced in: § A. Multilateral Instruments & Cross-border Cooperation

1. *See generally* Johnson & Post, *supra* § 2 A, note 31 (arguing that cyberspace cannot be governed by laws that rely on traditional territorial borders).

2. "Dual criminality" (also known as "double criminality") refers, in the context of international cooperation, to a requirement that the act subject to a request for extradition or MLA must be a criminal offence according to the criminal law of both not only the state making the request, but also according to the law of the state of which assistance is requested. *See, e.g.,* UNODC Cybercrime Study, *supra* § 1 C, note 7, at 202.

3. Amalie M. Weber, "The Council of Europe's Convention on Cybercrime," Berkeley Technology Law Journal, Vol. 18, (2003), p. 426, at http://scholarship.law.berkeley.edu/btlj/vol18/iss1/28

4. *See* US Dept. of State, Bureau of Counterterrorism, "Ch. 5: Terrorist Safe Havens" (listing certain "safe-havens"), in: *Country Reports on Terrorism* (2014), at http://www.state.gov/j/ct/rls/crt/2014/239412.htm.

5. At the same time, it is useful to consider the applicability of the United Nations Convention against Transnational Organized Crime (UNTOC), a global instrument reaching almost universal adherence with 187 States Parties, which takes into account "cyber" crimes committed by organized criminal groups.

6. *See* UNODC Cybercrime Study, *supra* § 1 C, note 7, at 67.

7. Some form of national cybercrime legislation exists in 149 countries, either in existing (137) or draft (24) form. *See, e.g.,* appendix 9 C.

8. *See, e.g.,* Zahid Jamil, "Cybercrime Model Laws: Discussion Paper Prepared for the Cybercrime Convention Committee (T-CY)," Council of Europe, (3 Dec. 2014), at https://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/3021_model_law_study_v15.pdf.

9. COMSEC, "Model Law on Computer and Computer Related Crime," in *2002 Meeting of Commonwealth Law Ministers and Senior Officials: Kingstown, St Vincent and the Grenadines, 18–21 November 2002,* (London: Commonwealth Secretariat,2003), at http://www.oecd-ilibrary.org/commonwealth/governance/2002-meeting-of-commonwealth-law-ministers-and-senior-officials/model-law-on-computer-and-computer-related-crime_9781848598188-16-en; COMSEC, "Draft Model Law on Electronic Evidence," in *2002 Meeting of Commonwealth Law Ministers and Senior Officials: Kingstown, St Vincent and the Grenadines, 18–21 November 2002,* (London: Commonwealth Secretariat, 2003), at http://www.oecd-ilibrary.org/commonwealth/governance/2002-meeting-of-commonwealth-law-ministers-and-senior-officials/draft-model-law-on-electronic-evidence_9781848598188-11-en; UN Conference on Trade and Development (UNCTAD) and Eastern African Community, "Draft EAC Legal Framework," (2008), at http://repository.eac.int:8080/bitstream/handle/11671/1815/EAC%20Framework%20for%20Cyberlaws.pdf?sequence=1&isAllowed=y; Common Market for Eastern and Southern Africa (COMESA), "Cybersecurity Draft Model Bill," (2011); ITU, "HIPSSA-Southern African Development Community Model Law on Computer Crime and Cybercrime," (2013); ITU, CARICOM & CTU, "Model Legislative Text on Cybercrime/e-Crimes and Electronic Evidence," (2010); ITU and Secretary of the Pacific Community, Model Law on Cybercrime, (2011). *See ibid,* for selected examples of implementation of non-binding multilateral instruments on cybercrime.

10. Of these multilateral treaties, only the AU Convention has not yet entered into force, as, *per* Article 36 of the Convention, the requisite threshold of fifteen ratifying AU Member States has not been achieved: to date, only eight Member States have signed the AU Convention, and none have ratified it. *See* "List of Countries Which Have Signed, Ratified/Acceded to the AU Convention," African Union, (1 Jun. 2016), at https://www.au.int/web/sites/default/files/treaties/29560-sl-african_union_convention_on_cyber_security_and_personal_data_protection.pdf.

11. UN Congress on Crime Prevention, *supra* § 2 A, note 3, at 15, (discussing recent developments in the use of science and technology by offenders and by competent authorities in fighting cybercrime).

12. Budapest Convention, *supra* § 1 B, note 32, at Preamble. Nine non-Member States of the CoE (Australia, Canada, Dominican Republic, Israel, Japan, Mauritius, Panama, Sri Lanka and the United States) have acceded to the Budapest Convention. *See* "Chart of Signatures and Ratifications of Treaty 185," CoE, at http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG. These countries were not all part of the process when provisions of the Convention were elaborated. A further thirteen countries (Argentina, Chile, Colombia, Costa Rica, Israel, Mexico, Morocco, Paraguay, Peru, Philippines, Senegal, Sri Lanka and Tonga), none of which are Member States of the Council of Europe, and none of which participated in the Convention's elaboration, have been invited to accede to this Convention.

13. *See supra* §§ 4 A & 4 B for a fuller discussion of the issues of safeguards, including due process issues, data protection, and access to information and freedom of expression.

14. *Ibid. See also* Budapest Convention, *supra* § 1 B, note 32, at Art. 15.

15. Budapest Convention, *supra* § 1 B, note 32, at Art. 15.

16. *Ibid.*, at Art. 37.1 ("the Committee of Ministers of the Council of Europe, after consulting with and obtaining the unanimous consent of the Contracting States to the Convention, may invite any State which is not a member of the Council and which has not participated in its elaboration to accede to this Convention").

17. "Chart of Signatures and Ratifications of Treaty 185," *supra* note 12.

18. *Ibid.*

19. *Ibid.*

20. CIS Agreement, *supra* § 2 A, note 47.

21. Budapest Convention, *supra* § 1 B, note 32 , at Art. 37.1.

22. CIS Agreement, *supra* § 2 A, note 47.

23. Budapest Convention, *supra* § 1 B, note 32.

24. The following are the twelve CIS Member States: Armenia, Azerbaijan, Belarus, Georgia, Kazakhstan, Kyrgyzstan, Moldova, the Russian Federation, Tajikistan, Turkmenistan, Ukraine and Uzbekistan.

25. The following are the six CIS Member States having ratified the CIS Agreement: Armenia, Azerbaijan, Belarus, Kazakhstan, Moldova and Tajikistan.

26. "Geneva Internet Platform," Digital Watch, at https://dig.watch/instruments/agreement-cooperation-combating-offences-related-computer-information-commonwealth.

27. SCO Agreement, *supra* § 2 A, note 62.

28. Budapest Convention, *supra* § 1 B, note 32; *see e.g.,* Constance Johnson, "Global Legal Monitor," US Library of Congress, at http://www.loc.gov/law/foreign-news/article/shanghai-cooperation-organization-agreements-signed/.

29. Budapest Convention, *supra* § 1 B, note 32, at Art. 37.1.

30. CIS Agreement, *supra* § 2 A, note 47.

31. SCO Agreement, *supra* § 2 A. note 62.

32. "About SCO," SCO, at http://rus.sectsco.org/about_sco/.

33. Arab Convention, *supra* § 2 A, note 14.

34. *Ibid.*, at Art. 1.

35. *Ibid.*, at Art. 4.1.

36. Budapest Convention, *supra* § 1 B, note 32, at Art. 37.1.

37. SCO Agreement, *supra* § 2 A, note 62, at Art.12.3, ("This Agreement, upon its entering into force, shall be open for accession by any State that shares the goals and principles of this Agreement.").

38. CIS Agreement, *supra* § 2 A, note 47, at Art. 17.

39. Arab Convention, *supra* § 2 A, note 14, at Ch. 5, Final Provision 4 (providing that "Any State of the League of Arab States that has not signed this Convention may accede to it").

40. *Ibid.*

41. AU Convention, *supra* § 2 A, note 48.

42. *See, e.g.,* Mailyn Fidler, "The African Union Cybersecurity Convention: A Missed Human Rights Opportunity," Council of Foreign Relations Blog, (22 Jun. 2015), at http://blogs.cfr.org/cyber/2015/06/22/the-african-union-cybersecurity-convention-a-missed-human-rights-opportunity/; Eric Tamarkin, "The AU's Cybercrime Response: A Positive Start, but Substantial Challenges Ahead," Institute for Security Studies, (Jan. 2015), at https://www.files.ethz.ch/isn/187564/PolBrief73_cybercrime.pdf.

43. *See* "List of Countries Which Have Signed, Ratified/Acceded to the AU Convention," *supra* note 10.

44. AU Convention, *supra* § 2 A, note 48, at Art. 36.

45. *See, e.g.,* Anahita Mathai, "The Budapest Convention and Cyber Cooperation," ORF Cyber Monitor, (12 Mar. 2015).

46. UNODC Cybercrime Study, *supra* § 1 C, note 7, at 199.

47. *Ibid.*, at 202.

48. Approximately 150 countries have domestic laws (either enacted or in draft) governing cybercrime. *See* appendix 9 C.

49. *See, e.g.,* ECOWAS, *Convention A/P.1/7/92 on Mutual Assistance in Criminal Matters,* at http://documentation.ecowas.int/download/en/legal_documents/protocols/Convention%20on%20Mutual%20Assistance%20in%20Criminal%20Matters.pdf; EU, "Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union," at http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=URISERV:l33108&from=EN; "SADC Protocol on Mutual Legal Assistance in Criminal Matters," SADC, at http://www.sadc.int/files/8413/5292/8366/Protocol_on_Mutual_Legal_Assistance_in_Criminal_Matters_2002.pdf.

50. UNODC Cybercrime Study, *supra* § 1 C, note 7, at xxv.

51. *Ibid.*

52. *Ibid.*, at 201.

53. *Ibid.*

54. Korean Criminal Act, *supra* § 2 E, note 14.

55. "Double Criminality Law & Legal Definition," US Legal.com, at http://definitions.uslegal.com/d/double-criminality/.

56. Urbas, *supra* § 2 E, note 53, at 12–13.

57. *See, e.g.,* Budapest Convention, *supra* § 1 B, note 32.

58. UNODC Cybercrime Study, *supra* § 1 C, note 7, at 206–07 (noting "the (often necessary) interplay between a range of government institutions can, in some cases, contributed to the long timescales reported for responses to requests").

59. Budapest Convention, *supra* § 1 B, note 32, at Art. 27.2.

60. CIS Agreement, *supra* § 2 A, note 47, at Art. 4.

61. Arab Convention, *supra* § 2 A, note 14, at Art. 34.2.

62. CIS Agreement, *supra* § 2 A, note 47, at Art. 6.2; Budapest Convention, *supra* § 1 B, note 32, at Art. 25.3 and 27.9; and Arab Convention, *supra* § 2 A, note 14, at Art. 32.3 and 34.8, respectively.

63. While not specific to the above-mentioned three multilateral treaties on cybercrime with fast means of communications for urgent MLA requests, UNODC provides as follows, "Being party to an international or regional instrument envisaging urgent mutual legal assistance channels appears to have a moderate effect – 55 percent of responding countries that were not party to any multilateral cybercrime instrument did not have channels for urgent requests, compared with 40 per cent of countries that were party to a multilateral cybercrime instrument." *See also* UNODC Cybercrime Study, *supra* § 1 C, note 7, at 207–208.

64. Budapest Convention, *supra* § 1 B, note 32, at Preamble.

65. *Ibid.*, at Art. 22.3. With regard to offenses committed by the national of a state, the Convention is only applicable if the offense is criminally punishable where committed, or if the offense is committed outside the territorial jurisdiction of any state (thereby avoiding the possibility of negative jurisdiction). *Ibid.,* at Art. 22.3.d.

66. *Ibid.*, at Art.22.4.

67. *Ibid.*, at Art. 14–15 (discussing the scope of, and safeguards for, these tools).

68. States bound by the European Convention on Human Rights violate their duty to their citizens and victims' human rights if privacy laws prevent law enforcement authorities from conducting adequate electronic investigations in criminal cases. *K.U. v. Finland,* 2872/02 [2008] ECtHR 1563, at http://www.echr.coe.int/Documents/Reports_Recueil_2008-V.pdf. Although this is a ECtHR decision, it is instructive for other regions.

69. Budapest Convention, *supra* § 1 B, note 32, at Art. 25.

70. *See, e.g., ibid.,* at Art. 22 & 24 (especially noting at Art. 24.1.3, "If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article.").

71. Oxford Dictionary of Law.

72. "The Obligation to Extradite or Prosecute" ("aut dedere aut judicare"), Final Report of the UN International Law Commission, (2014), at http://legal.un.org/ilc/texts/instruments/english/reports/7_6_2014.pdf; Budapest Convention, *supra* § 1 B, note 32, at Art. 24.6. *See also* Budapest Explanatory Report, *supra* § 1 D, note 14, at para. 251.

73. *See, e.g.,* Urbas, *supra* § 2 E, note 53, at 13–14.

74. European Convention on Extradition, Paris, ETS No. 24 (13 Dec. 1957), Arts. 3 & 11, at https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/024.

75. *See, e.g., Lazar, supra* § 2 B, case 2.2.

76. *See, e.g.,* Budapest Convention, *supra* § 1 B, note 32, at Art. 24. Dual criminality is intended to protect individuals from state persecution for political crimes.

77. *Ibid.,* at Art. 22 & 24.

78. *Ibid.,* at Art. 24.1.b.

79. *See* Budapest Explanatory Report, *supra* § 1 D, note 14, at para. 245.

80. *Ibid.*

81. Budapest Convention, *supra* § 1 B, note 32, at Art. 24.1.

82. Amalie M. Weber, "The Council of Europe's Convention on Cybercrime," Berkeley Technology Law Journal, Vol. 18 (2003), p. 426, at http://scholarship.law.berkeley.edu/btlj/vol18/iss1/28.

83. *See, e.g.,* Statement of US Attorney General Alberto R. Gonzales on the Passage of the Cybercrime Convention, US Dept. of Justice, at http://www.justice.gov/archive/opa/pr/2006/August/06_ag_499.html ("This treaty provides important tools in the battles against terrorism, attacks on computer networks and the sexual exploitation of children over the Internet, by strengthening U.S. cooperation with foreign countries in obtaining electronic evidence.").

84. Walden, *supra* § 2 A, note 67.

Referenced in: § B. Establishing Informal International Cooperation

1. UN General Assembly, "Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, 68th Plenary Meeting," (14 Dec. 1990), at http://www.un.org/documents/ga/res/45/a45r121.htm.

2. Weiping Chang, Wingyan Chung, Hsinchun Chen & Shihchieh Chou, "An International Perspective on Fighting Cybercrime," ISI'03 Proceedings of the 1st NSF/NIJ Conference on Intelligence and Security Informatics, (2003).

3. ITU, "Geneva Declaration of Principles and the Geneva Plan of Action," (Geneva: ITU, 2003), para. 35–37, at https://www.itu.int/net/wsis/docs/promotional/brochure-dop-poa.pdf.

4. *See supra* § 3 A.

5. Budapest Convention, *supra* § 1 B, note 32.

6. The Budapest Convention, though perhaps the most visible instrument, is not the only one. *See* EU *Convention on Simplified Extradition Procedure Member States,* Council Act of 10 March 1995, OJ C 78 (30 Mar. 1995).

7. For instance, even before the Budapest Convention, the European Union had been encouraging its member States to enact national legislation to facilitate mutual legal assistance in the search and seizure of evidence from organized crime and high-tech crime. *See e.g.,* EU, *Act of 12 March 1999 on Adopting the Rules Governing the Transmission of Personal Data by Europol to Third States and Third Bodies,* OJ C 088 (30 Mar. 1999), at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31999F0330. *See also* EU Council *Resolution of 17 Jan. 1995, on the Law Interception of Telecommunications,* OJ C 329 (11 Nov. 1996), at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31996G1104.

8. *See e.g.,* Budapest Convention, *supra* § 1 B, note 32; EU, *Joint Action of 29 Nov. 1996 adopted by the Council on the Basis of Article K.3 of the Treaty on European Union, Concerning the Creation and Maintenance of a Directory of Specialized Competences, Skills, and Expertise in the Fight against International Organized Crime, in Order to Facilitate Law Enforcement Cooperation between the Member States of the European Union,* 96/747/JHA (29 Nov. 1996), at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31996F0747; EU, *Joint Action of 29 Jun. 1998 Adopted by the Council on the Basis of Article K.3 of the Treaty on European Union, on Good Practice in Mutual Legal Assistance in Criminal Matters,* OJ L 191 (7 Jul. 1998), pp. 1–3, at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31998F0427; EU, *Act of the Management Board of Europol of 15 Oct. 1998 concerning the Rights and Obligations of Liaison Officers,* OJ C 026 (30 Jan. 1999), pp. 86–88, at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31999F0130(08); and the EU, *Draft Council Act Establishing the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union,* OJ C 251 (2 Sep. 2, 1999), at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A51999AG0902(01).

9. *See, e.g.,* "The G8 24/7 Network of Contact Points, Protocol Statement," Organization of American States (OAS), (2007), p. 2, at http://www.oas.org/juridico/english/cyb_pry_G8_network.pdf.

10. A multilateral political forum, the G8 addresses a wide range of international economic, political, and security issues. It is formed of representation from eight countries, with responsibility for hosting the G8 rotating through the Member States in the following order: France, United States, United Kingdom, Russia, Germany, Japan, Italy and Canada. The European Commission attends G8 meetings as an observer. Although, with Russia's 2014 suspension (following its annexation of Crimea), the G8 was reduced in number and became the G7, the 24/7 Network remains named after the G8, though membership is open to all. Alison Smale & Michael D. Shearmarch, "Russia Is Ousted from Group of 8 by US and Allies," New York Times, (24 Mar. 2014), at http://www.nytimes.com/2014/03/25/world/europe/obama-russia-crimea.html?_r=0.

11. This subgroup, often referred to as the Roma-Lyon group, is the result of a meeting in Rome in October 2001 of senior representatives of G8 Justice and Home Affairs Ministries to discuss steps for the G8 to take to combat international terrorism, and which combined the G8's Lyon Group (fighting transnational organized crime) and the G8's Roma Group (fighting international terrorism). *See* "G8 Background," US Dept. of Justice, (11 May 2004), at https://www.justice.gov/ag/g8-background. While continuing important work to combat transnational organized crime, the group uses its resources to combat terrorism through such avenues as enhancements to legal systems, transport security and tools for investigating terrorist uses of the internet. *Ibid.*

12. With the goal of ensuring that no criminal receives safe havens anywhere in the world, the G8 States established the Subgroup of High-Tech Crime in 1997 at a meeting in Washington, DC, adopting Ten Principles in the combat against computer crime, G8, "The Washington Communiqué," Meeting of Justice and Interior Ministers of the Eight, (10 Dec. 1997), at https://www.justice.gov/sites/default/files/ag/legacy/2004/06/08/97Communique.pdf.

13. "G8 – 24/7 Network," Organization of American States (OAS), at http://www.oas.org/juridico/english/cyber_g8.htm.

14. Global Monitoring and ECPAT International, *Status of Action against Commercial Sexual Exploitation of Children: Israel (2016),* (Bangkok: ECPAT International, 2016), at http://www.ecpat.org/wp-content/uploads/2016/06/A4A_V1_ISARAEL_2016June.pdf.

15. *See, e.g.,* Kjell Engelbrekt, *High-Table Diplomacy: The Reshaping of International Security Institutions,* (Washington, DC: Georgetown University Press, 2016), p. 135. *See also* "G8 Declaration Renewed Commitment For Freedom And Democracy," G8 Summit of Deauville, (26–27 May 2011), at http://www.nato.int/nato_static/assets/pdf/pdf_2011_05/20110926_110526-G8-Summit-Deauville.pdf.

16. *See, e.g.,* Office of the Spokesperson, "Media Note: G8 Foreign Ministers' Meeting Statement," US Dept. of State, (11 Apr. 2013), at http://www.state.gov/r/pa/prs/ps/2013/04/207354.htm.

17. Budapest Convention, *supra* § 1 B, note 32, at Art. 35.

18. *Ibid.*

19. *Ibid.*, at Art. 35.1(a–c).

20. *Ibid.*, at Art. 35.

21. "Assistant Attorney General Leslie R. Caldwell Speaks at the CCIPS-CSIS Cybercrime Symposium 2016: Cooperation and Electronic Evidence Gathering Across Borders," US Dept. of Justice, (6 Jun. 2016), at https://www.justice.gov/opa/speech/assistant-attorney-general-leslie-r-caldwell-speaks-ccips-csis-cybercrime-symposium-2016.

22. "Data Exchange," INTERPOL, at http://www.interpol.int/INTERPOL-expertise/Data-exchange/I-24-7. There are 190 INTERPOL member countries. *See* "World: A Global Presence," INTERPOL, at http://www.interpol.int/Member-countries/World.

23. *Ibid.*

24. *Ibid.*

25. "Hacker Demands Money for Information on S. Korean Nuclear Reactors," Yonhap, (12 Mar. 2015), at http://english.yonhapnews.co.kr/national/2015/03/12/40/0302000000AEN20150312008051320F.html; Justin McCurry, "South Korean Nuclear Operator Hacked Amid Cyber—Attack Fears," Guardian, (23 Dec. 2014), at https://www.theguardian.com/world/2014/dec/22/south-korea-nuclear-power-cyber-attack-hack; Sohee Kim & Meeyoung Cho, "South Korea Prosecutors Investigate Data Leak at Nuclear Power Plants," Reuters, (21 Dec. 2014), at http://www.reuters.com/article/us-southkorea-nuclear-idUSKBN0JZ05120141221.

26. *Ibid.*

27. Caroline Baylon, Roger Brunt & David Livingstone, "Cyber Security at Civil Nuclear Facilities Understanding the Risks," Chatham House, (Sep. 2015), at https://www.chathamhouse.org/sites/files/chathamhouse/field/field_document/20151005CyberSecurityNuclearBaylonBruntLivingstone.pdf.

28. Pierluigi Paganini, "South Korea—Hacker Requests Money for Data on Nuclear Plants," Security Affairs, (18 Mar. 2015), at http://securityaffairs.co/wordpress/35013/cyber-crime/hacker-south-korean-nuclear-plants.html.

29. *See supra* table 5.1.

30. UNODC Cybercrime Study, *supra* § 1 C, note 7, at 124–25.

31. "The INTERPOL Global Complex for Innovation," INTERPOL, at http://www.interpol.int/About-INTERPOL/The-INTERPOL-Global-Complex-for-Innovation/About-the-IGCI.

32. It bears noting that INTERPOL's then-president, Khoo Boon Hui (2008–2012), is Singaporean. *See* "Khoo Boon Hui," INTERPOL, at http://www.interpol.int/About-INTERPOL/Structure-and-governance/KHOO-Boon-Hui.

33. *See* "Structure and Governance," INTERPOL, at http://www.interpol.int/About-INTERPOL/Structure-and-governance/General-Secretariat.

34. *See* "Command and Coordination Centre—Aires," INTERPOL, at http://www.interpol.int/INTERPOL-expertise/Command-Coordination-Centre/Command-and-Coordination-Centre-Buenos-Aires.

35. INTERPOL's Secretariat has seven regional offices: (1) Buenos Aires, Argentina; (2) Yaoundé, Cameroon; (3) Abidjan, Côte d'Ivoire; (4) San Salvador, El Salvador; (5) Nairobi, Kenya; (6) Bangkok, Thailand; and (7) Harare, Zimbabwe.

36. "European Cybercrime Center," Europol, at https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3.

37. "Combating Cybercrime in a Digital Age," Europol, European Cybercrime Centre (EC3), at https://www.europol.europa.eu/ec3.

38. *Ibid.*

39. *Ibid.*

40. "Joint Cybercrime Action Taskforce (J-CAT)," Europol, European Cybercrime Centre (EC3), at https://www.europol.europa.eu/ec3/joint-cybercrime-action-taskforce-j-cat.

41. *Ibid.*

42. "History of Eurojust," Eurojust, at http://www.eurojust.europa.eu/about/background/Pages/history.aspx.

43. EU, *Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community*, (13 Dec. 2007) 2007/C 306/01 [hereafter, "Lisbon Treaty"], Ch. 4, Art. 85, at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3Aai0033.

44. "Mission and Tasks," Eurojust, at http://www.eurojust.europa.eu/about/background/Pages/mission-tasks.aspx.

45. "History of Eurojust," *supra* note 42.

46. Contact points in non-Member States include Albania, Argentina, Bosnia and Herzegovina, Canada, Egypt, the former Yugoslav Republic of Macedonia, Iceland, Israel, Japan, Korea, Liechtenstein, Moldova, Mongolia, Montenegro, Norway, the Russia, Serbia, Singapore, Switzerland, Thailand, Turkey, Ukraine and the United States. Korea is the most recent addition. *See* "Mission and Tasks," *supra* note 44.

47. *Ibid.*

48. Judicial Network & Eurojust, "Joint Task Force Paper Assistance in International Cooperation in Criminal Matters for Practitioners European," Press Release, Council of the European Union, (6 May 2014), at http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressdata/en/jha/104584.pdf.

49. For details about Global Prosecutors E-Crime Network (GPEN), *see* "Global Prosecutors E-Crime Network," International Association of Prosecutors, (11 Jun. 2012), at https://rm.coe.int/CoERMPublicCommonSearchServicesDisplayDCTMContent?documentId=09000016802f240e.

50. "History of Eurojust," *supra* note 42.

51. "Mission and Tasks," *supra* note 44.

52. *Ibid.*

53. *Ibid.*

54. *Ibid.*

55. "Operation BlackShades: An Evaluation," Eurojust, (2015), at https://www.gccs2015.com/sites/default/files/documents/Bijlage%202%20-%20Eurojust%20(10%2004%2015)%20Blackshades-Case-Evaluation.pdf.

56. "International Blackshades Malware Takedown-Coordinated Law Enforcement Actions Announced," FBI, (2014), at https://www.fbi.gov/news/stories/international-blackshades-malware-takedown-1.

57. "Operation BlackShades: An Evaluation," *supra* note 55.

58. *Ibid.*

59. *Ibid.*

60. *Ibid.*

61. *Ibid.*

62. "National Cyber-Forensics and Training Alliance," NCFTA, at http://www.ncfta.net/.

63. *See* "Who We Are," NCFTA, at http://www.ncfta.net/.

64. *See* "Agencies," US Dept. of Justice, at https://www.justice.gov/agencies.

65. *See* "About InfraGard," InfraGard, at https://www.infragard.org/.

66. *See* "NCFTA in the News: The National Cyber-Forensics and Training Alliance to Open New Offices in Los Angeles and New York," NCTFA, (8 Jan. 2016), at https://www.ncfta.net/Home/News.

67. *See* "NCFTA in the News: International Alliance Against Counterfeiting," NCTFA, (18 Jul. 2016), at https://www.ncfta.net/Home/News.

68. "Who We Are," NCFTA, *supra* note 63.

69. For a further discussion of cooperation between the public and private sector, *see infra* § 6 F.

70. "CyFin," NCFTA, at http://www.ncfta.net/Home/Cyfin.

71. "BCP," NCFTA, at http://www.ncfta.net/Home/BCP.

72. "MCT," NCFTA, at http://www.ncfta.net/Home/Malware.

73. For a further discussion of cooperation between the public and private sector, *see infra* § 6 F.

74. "Commonwealth Cybercrime Initiative," The Commonwealth, at http://thecommonwealth.org/commonwealth-cybercrime-initiative.

75. "The Commonwealth Cybercrime Initiative: A Quick Guide," The Commonwealth (2014), at http://www.securityskeptic.com/CCI%20Quick%20Guide.pdf.

76. *Ibid.*, "Commonwealth Cybercrime Initiative," *supra* note 74.

77. *See supra* § 3 A for further discussion of the Harare Scheme.

78. "Communiqué: Commonwealth Law Ministers Meeting," The Commonwealth, (5–8 May 2014), para. 14, at http://thecommonwealth.org/media/news/communique-commonwealth-law-ministers-meeting-2014#sthash.oZZBUeVU.dpuf.

79. CCI was created in 2011 under the auspices of the Commonwealth Connects program that was created by the Heads of Government during their 2005 meeting in Malta to bridge the digital divide. CCI was formally endorsed by the Commonwealth Heads of Government Meeting (CHOGM) during their 2011 meeting in Perth, Australia.

80. "Commonwealth Cybercrime Initiative," *supra* note 74.

81. Executive Management Committee (EMC) Country Members include Canada, India, Malta, New Zealand, Trinidad & Tobago, Uganda and the United Kingdom (current chair); EMC Institutional Members include COMSEC, ComNet, Interpol and ICANN; the US Dept. of State is an EMC Observer. *See* "The Commonwealth Cybercrime Initiative: A Quick Guide," supra note 75.

82. COMSEC, *ibid.*

83. "Commonwealth Cybercrime Initiative," *supra* note 74.

84. *Ibid.*

85. *Ibid.*

86. Carolin Weisser, "Eastern African Criminal Justice Network on Cybercrime and Electronic Evidence," Cybersecurity Capacity Portal, Oxford University, (4 Nov. 2015), at https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/eastern-african-criminal-justice-network-cybercrime-and-electronic-evidence.

87. *See* CCI, "Gros Islet Communiqué," The Caribbean Stakeholders Meeting on Cybersecurity and Cybercrime (CSM-II), (16–18 Mar. 2016), at http://thecommonwealth.org/sites/default/files/news-items/documents/6%20FinalCastriesDeclaration170316.pdf; "Caribbean to Tackle Escalating Cybercrime with Regional Approach," The Commonwealth, (15 Mar. 2016), at http://thecommonwealth.org/media/press-release/caribbean-tackle-escalating-cybercrime-regional-approach#sthash.HjmhE8I8.dpuf.

88. "Who We Are," OAS, at http://www.oas.org/en/about/who_we_are.asp.

89. OAS General Assembly, *The Inter-American Integral Strategy to Combat Threats to Cyber Security,* (8 Jun. 2004) AG/RES.2004 (XXXIV-O/04).

90. The topic of cyberterrorism is beyond the scope of the Toolkit. Nonetheless, it bears noting that the lines between acts of cybercrime and cyberwar or cyberterrorism are increasingly blurred, especially, as the World Development Report has noted, "acts that might previously have been considered civilian attacks are now being uncovered as acts of states against states via nonstate actor proxies." *See* WDR, *supra* § 1 A, note 10, at 222.

91. "Cyber Security," OAS, at https://www.sites.oas.org/cyber/en/Pages/default.aspx.

92. "Best Practices for Establishing a National CSIRT," OAS, (2016), at https://www.sites.oas.org/cyber/Documents/2016%20-%20Best%20Practices%20CSIRT.pdf.

93. Inter-American Cooperation Portal on Cyber-Crime, "Welcome," OAS, at http://www.oas.org/juridico/english/cyber.htm.

94. *Ibid.*

95. *See e.g.,* "Progress Report 2013-2014," Internet & Jurisdiction, (2014), at http://www.internetjurisdiction.net/uploads/pdfs/Annual-Reports/Internet-Jurisdiction-2013-14-Report.pdf.

96. *Schrems v. Data Protection Commissioner,* CJEU, Case C-362/14 (6 Oct. 2015), at http://curia.europa.eu/juris/document/document.jsf?docid=169195&doclang=EN; *See also* CJEU, "The Court of Justice Declares That the Commission's US Safe Harbour Decision Is Invalid," Press Release, (6 Oct. 2015), at http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf.

97. *See e.g.,* Dave Lee, "How Worried Is Silicon Valley about Safe Harbour?," BBC News, (7 Oct. 2015), at http://www.bbc.com/news/technology-34461682; Kelli Clark, "The EU Safe Harbor Agreement Is Dead, Here's What To Do about It," Forbes, (27 Oct. 2015), at http://www.forbes.com/sites/riskmap/2015/10/27/the-eu-safe-harbor-agreement-is-dead-heres-what-to-do-about-it/#2f3bd6757171; Kolvin Stone, Christian Schröder, Antony P. Kim & Aravind Swaminathan, "US–EU Safe Harbor – Struck Down!," Orrick Trust Anchor Blog, (6 Oct. 2015), at http://blogs.orrick.com/trustanchor/2015/10/06/us-eu-safe-harbor-struck-down/.

98. European Commission, "EU Commission and United States Agree on New Framework for Transatlantic Data Flows: EU-US Privacy Shield Strasbourg," Press Release, (2 Feb. 2016), at http://europa.eu/rapid/press-release_IP-16-216_en.htm.

99. European Commission, "EU-US Privacy Shield: Frequently Asked Questions," Fact Sheet, (12 Jul. 2016), at http://europa.eu/rapid/press-release_MEMO-16-2462_en.htm.

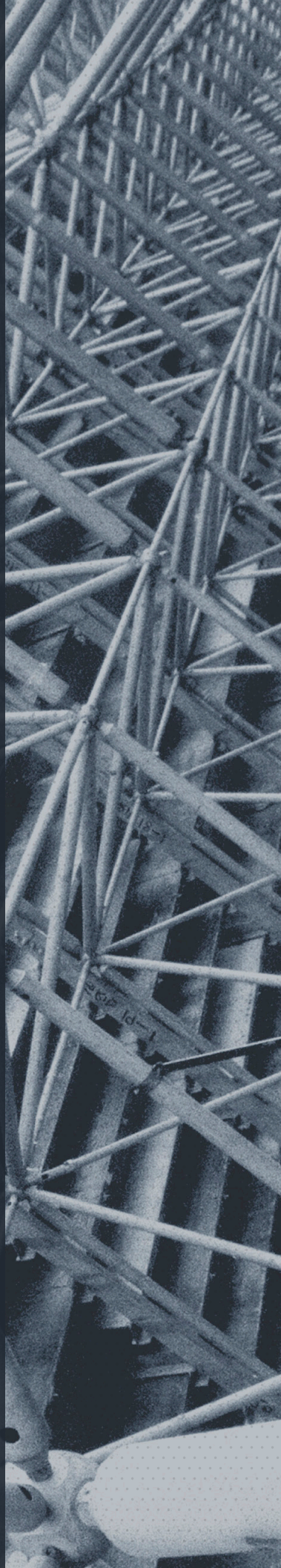
100. For various T-CY CoE reports, *see* "T-CY Reports," CoE, at http://www.coe.int/en/web/cybercrime/t-cy-reports.

CHAPTER 6

Capacity Building

This chapter provides an overview of some capacity-building issues starting by looking at capacity building for policy makers and legislators, law enforcement, consumers and cooperation with the private sector, as well as highlighting activities of the participating organizations.

In this Chapter



A. The Capacity-building Challenge

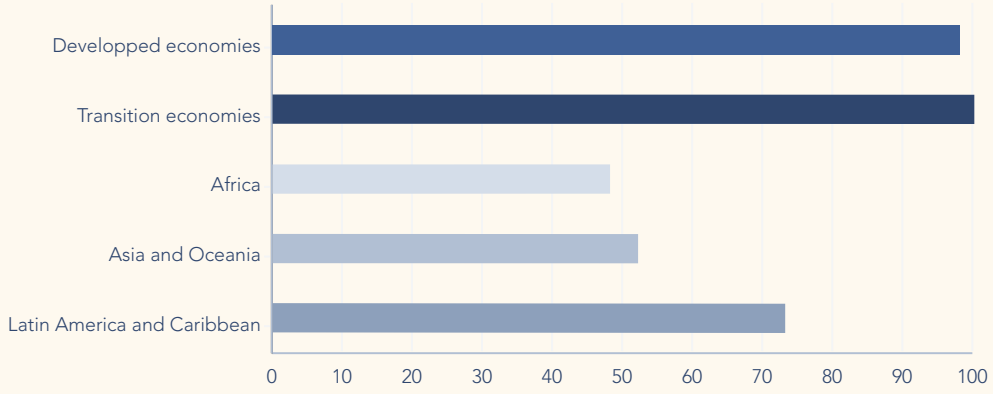
Table of Contents

Introduction

Addressing security concerns related to ICTs is of growing importance for governments, as well as for both regional and international organizations involved in creating a safe, digital environment by building confidence in online transactions. As a consequence, an increasing number of countries have adopted or strengthened their cybercrime legislation.

According to the *UNCTAD Global Cyberlaw Tracker,*[1] 138 states have adopted a law on cybercrime and fourteen have a draft law. Figure 6.1 shows that the adoption of cybercrime legislation is fairly widespread across developed and transition economies, but less so in Africa and Asia.

Figure 6.1: Cybercrime Legislation Adoption Worldwide (percentage)[2]



The development of domestic legal frameworks for combating cybercrime should not be done in isolation. It is essential that the interoperability of such laws and policies at the regional and international level be assured. Establishing common minimum standards can help ensure cross-border coordination on the design and implementation of relevant legislation and enforcement mechanisms. As already discussed, the judiciary and the police would benefit from cooperating with their colleagues at the international level (*see* section 5 B, above).

Once the legal framework has been prepared, the onus falls to the implementers to realize effective enforcement regimes. Cybercrime's facility for crossing borders, especially once combined with the ability of cybercriminals to operate anonymously and to act both from and through multiple jurisdictions, makes the need for strong, cooperative law enforcement mechanisms even more urgent. Furthermore, governments should strive to reinforce the human, procedural and technical resources needed both to collect and analyze evidence, and to identify and prosecute cybercriminals as part of an intergovernmental prosecutorial effort.

I. Barriers to Interoperability

The main barriers to the development of cybercrime laws faced by governments worldwide, especially in developing countries include:

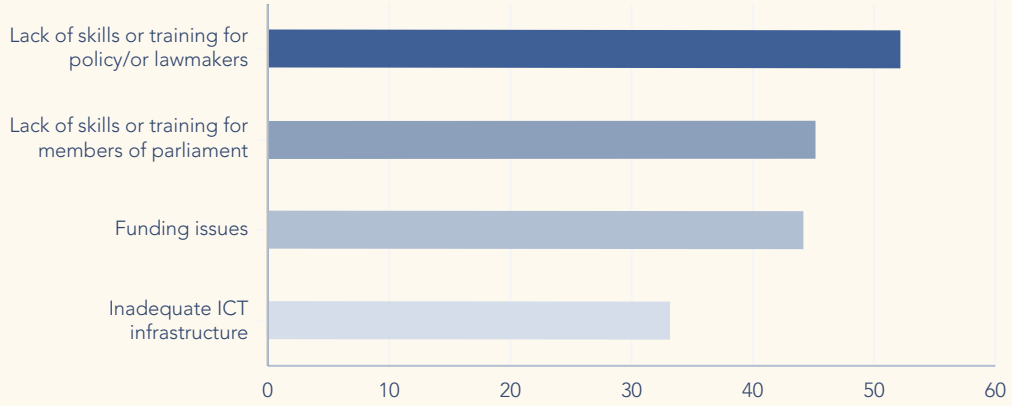
1. Stakeholders possibly affected by cyberlaw have limited understanding and experience with such legislation.
2. Cyberlaw may be developed in a number of different ways, and implemented in various stages, all of which has varying costs, and which is affected, and often delayed, by a scarcity of both human and financial resources.

3. Developing legislation takes time, may progress slowly, and may be prolonged due to numerous factors, most notably by the stakeholder consultation processes, which is complicated by the wide range of stakeholders, but which is essential to building consensus before formal introduction and implementation.
4. Enforcing and prosecuting cybercrime is particularly difficult.

The need for policy and law-makers to understand cybercrime issues and their multinational dimension is present in all countries. An UNCTAD survey, with responses from government representatives in forty-eight developing countries, emphasized a need to build awareness and knowledge among lawmakers and judiciary bodies with regard to cybercrime law and enforcement policy (see figures 6.2 and 6.3).

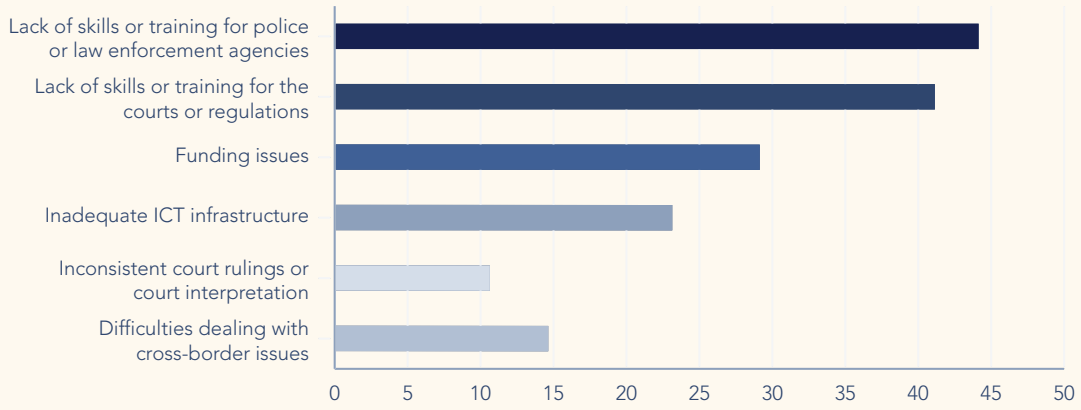
Over half of the representatives reported difficulties in understanding legal issues related to cybercrime. Similarly, over forty percent noted that lack of understanding among parliamentarians can delay the adoption of relevant laws. Without awareness and knowledge, it is difficult to formulate informed policies and laws and to enforce them.

Figure 6.2: Challenges to the Enactment of e-Commerce Legislation in the ASEAN, ECOWAS and Selected Latin America and Caribbean Countries, 2013-2015 (Percentage of Respondents)[3]



Other challenges include the need for informed regulators and for training law enforcement bodies, as well as sufficient resources to create effective legal frameworks and national certification authorities.

Figure 6.3: Challenges to the Enforcement of e-Commerce Legislation in the ASEAN and Selected Latin America and Caribbean Countries, 2013-2015 (Percentage of Respondents)[4]



The implementation of cybercrime legislation is always challenging, especially in countries where resources (both in terms of skills and security systems) are insufficient. While adequate laws and technology are essential for the provision of protection against information security risks, they need to be complemented by adequate and relevant expertise.

With regard to the security of communications infrastructure, national and international coordination and cooperation on matters of access to data and communications are important. In order to act effectively upon criminal procedural needs of specific cases, it is critical that law enforcement have the capacity to execute searches and seizures and intercept communications—and to do so across several jurisdictions. Nonetheless, a large number of countries are facing challenges in understanding the issues at stake and combating cybercrime.

A coherent strategy to address these issues is required; such a strategy should aim to:

1. Make the fight against cybercrime a priority and allocate the necessary financial resources; and
2. Assess shortcomings in terms of infrastructure and human capacity.

With regard to human capacity, relevant stakeholders who play, or should play, a role in cybersecurity management should be identified. They usually include policy makers, law makers, and law enforcers such as judges and magistrates, police officers and CERT officers. Training and briefing initiatives can be designed based on the category, number and individual needs of each group of stakeholders. For example, policy and law makers, including parliamentarians, need to understand cybercrime and cyberlaw in general, their application and impact. Training workshops can be organized at the government level, involving various ministries/institutions for two to five

days, while for parliamentary committees members, a general briefing on cybercrime issues and of cyberlaw and its application and impact over half a day or one-day maximum.

For judges, magistrates and prosecutors—those who need to implement the law and legal regime—the capacity-building might be done two in phases:

- **Phase 1**
  - Overview on the legal implications on cybersecurity to criminal laws and other related laws;
  - Overview on the legal framework on cybercrimes and other related emerging issues;
  - Legal issues information security, data protection and security standards;
  - Legal issues on cybersecurity and nature of cybercrimes, children protection online; and
  - Other criminal activities associated with the use of computers.
- **Phase 2**
  - Cybercrime prosecution;
  - Computer privacy and data protection principles/cross-border data flows;
  - Legal issues on admissibility of e-evidence;
  - Judicial considerations and case studies; and
  - Criminal law and copyright law (piracy and other related offences).

II. Mapping Technical Assistance Needs

A useful process to identify needs to be addressed through technical assistance is through the development of indices for assessing relevant threats, national measures to address them, as well as initiatives of organizations. In addition to the Assessment Tool featured in chapter 7, a variety of other tools are available to map technical assistance needs.

One such example is the ITU Global Cybersecurity Index (GCI), which measures the cybersecurity commitment of Member States with regards to the five pillars endorsed by the Global Cybersecurity Agenda (GCA), namely the ITU framework for international multi-stakeholder cooperation in cybersecurity aimed at building synergies with current and future initiatives and focuses on the following five work areas:

- Legal measures;
- Technical and procedural measures;
- Organizational structures;

- Capacity-building; and
- International cooperation.

The objective of the GCI initiative is to help countries identify areas for improvement in the field of cybersecurity, as well as to motivate them to take action to improve their ranking, thus helping raise the overall level of cybersecurity worldwide. Through the collected information, GCI aims to illustrate the practices of others so that Member States can implement selected aspects suitable to their particular national environment, with the added benefit of helping harmonize practices and foster a global culture of cybersecurity.

A first iteration of the GCI was conducted in 2014 in partnership with ABI Research and the final results have been published.[5] A total of 105 of 193 ITU Member States responded. Secondary data was used to build the index for non- respondents. In parallel, "cyberwellness" profiles of all states were elaborated and are accessible from the GCI website. These profiles are factual representations of cybersecurity actions and planned initiatives by each state. The profiles, unlike the GCI, can be updated at any point in time at the request of the states and are thus considered as live up-to-date documents.

GCI 2017 was released in June 2017 and updates and expands the data gathered in the first iteration of the GCI in 2014.[6] A total of 134 countries out of 193 ITU Member States responded to the questionnaire. Secondary data was used to build the index for non-respondents. A number of new questions were added in each of the five pillars in order to refine the depth of research.

III. UNODC Cybercrime Repository

UNODC recently released its Cybercrime Repository, a central data repository of cybercrime laws and lessons learned for the purposes of facilitating the continued assessment of needs and criminal justice capabilities and the delivery and coordination of technical assistance.[7] UNODC started developing its Cybercrime Repository in early 2014 pursuant to resolution 22/8 of the Commission on Crime Prevention and Criminal Justice (CCPCJ). The rationale behind the mandate was to make the comprehensive data sets gathered for its Comprehensive Study on Cybercrime via Member State questionnaires accessible to a wider audience.[8]

The repository contains a Case Law Database, a Database of Legislation and a Lessons Learned Database. The first two databases are the same databases as contained in the SHERLOC portal, a UNODC knowledge management portal aimed at facilitating the dissemination of information regarding the implementation of the UN Convention against Transnational Organized Crime[9] and its three Protocols, as well as new and emerging forms of crime and their links to transnational organized crime.

The repository, which was officially launched in May 2015 during a side event at the CCPCJ, contains the following three types of information that are especially pertinent to e-commerce:

- National cybercrime and cybersecurity strategies (based on desk research);
- National cybercrime lead agencies (as provided by Member States); and
- Lessons learned—cybercrime policies and strategies, as well as good practices in cybercrime investigation, prosecution and prevention (as provided by Member States via questionnaire for the Comprehensive Study on Cybercrime and via Note Verbale in the form of short texts).

IV. ICT-facilitated Child Sexual Abuse & Sexual Exploitation

While the 2013 UNODC Comprehensive Study on Cybercrime revealed that the criminal misuse of ICT can take many forms, it produced additional evidence showing that children are particularly at risk of becoming victims of ICT-facilitated crimes. The fundamental issue is that children often do not fully understand the threats associated with sharing personal information, photos or videos, nor fully comprehend the facility with which that information can be accessed anonymously.

In light of the above, the UN Economic and Social Council adopted resolution 2011/33, entitled "Prevention, protection and international cooperation against the use of new information technologies to abuse and/or exploit children".[10] This resolution mandated the elaboration of a UNODC Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children, which was duly completed in 2015.[11] This later UNODC Study is intended to promote the exchange of experience and good practices in an effort to address the growing problem of ICT-facilitated child sexual abuse and exploitation.

Findings contained in this Study point to the fact that ICTs can be used both to commit already known forms of child abuse and exploitation and to engage in new forms of child abuse and exploitation. In addition, the use of ICTs for the commission of these acts leads to the continuing victimization of children by facilitating the interlinking of crimes, for example through the production of child sexual abuse material and then through the distribution and possession of such material.

Through their use of the internet, children may be exposed to other forms of abuse such as grooming, solicitation, stalking, harassment, bullying and exposure to harmful content. Organized criminal networks have much to gain in financial terms from the use of ICTs in the commission of child abuse and exploitation. Moreover, the accessibility of these relatively inexpensive technologies means that collaboration across borders among organized criminal groups is prevalent.

Bearing the above in mind, it is imperative for governments and other partners to develop enhanced international cooperation and prevention strategies, as well as more targeted law enforcement techniques.

As affirmed by the UN Economic and Social Council,[12] children should be afforded the same protection in cyberspace as they are in the physical world. To this end, legislation, including necessary criminal provisions, needs to be developed or upgraded, and efficiently implemented, principally by national authorities but also in consultation with other partners, such as civil society and the private sector. Technical capacities for law enforcement, including access to technological tools, need to be strengthened in order to detect, investigate and secure evidence of related offences.

The UNODC Study provides a global picture of the issues at stake and further defines the typology of the crimes that need to be addressed, as well as the appropriate responses at national and international levels. It was based on open-source research on the issue, as well as the work of a UNODC Informal Expert Group Meeting on the subject, which was convened in Vienna from 23 to 25 September 2013, and which brought together experts from international organizations, law enforcement, other relevant practitioners and academics. The Study also forms part of UNODC's technical assistance tools in the area of prevention and combatting of cybercrime.

V. Addressing the Capacity-building Challenge

Addressing the capacity-building challenge requires **(A)** a general understanding of the diverse capacity-building issues before **(B)** a more targeted understanding of how internal capacity can be built to, specifically, improve international cooperation and before **(C)** discussing the place for knowledge sharing and dissemination at all levels, including citizen awareness.

A. General Capacity-building Issues

Policy and law makers, as well as criminal justice and law enforcement personnel, especially in developing countries, need training in combating cybercrime, especially in developing countries. Capacity-building at the level of national law enforcement and criminal justice systems, in particular, is critical. While the majority of countries have begun to put in place specialized structures for the investigation of cybercrime and crimes involving e-evidence, in many countries those structures are underfunded and suffer from a lack of capacity. As e-evidence becomes increasingly pervasive in investigating "conventional" crimes, law enforcement authorities may need to make clear distinctions between cybercrime investigators and digital forensic laboratory capacity, establishing clear workflows. Frontline law enforcement officers may also increasingly need to acquire and deploy basic skills, such as those used to produce a sound forensic image of an electronic storage device.

Moreover, as new technological developments such as anonymizing networks, high-grade encryption and virtual currencies become commonplace in cybercrime, investigators will also have to adopt new strategies. Law enforcement authorities may, for example, look to strengthen

partnerships with academic research groups that focus on the development of technical methodologies in areas such as the characterization and investigation of virtual currency transactions.

Investigators may also need to consider how special investigative techniques, such as surveillance, undercover operations, using informants and controlled delivery in the case of the online sales of illicit goods, might be used alongside internet investigations and digital forensic techniques.

Overall, it is clear that capacity-building for law enforcement and criminal justice actors on combating cybercrime will be an ongoing and continuous process, as technology and criminal innovations continue at a rapid pace.

B. Increasing Internal Capacity to Improve International Cooperation

A specific area of technical assistance to which UNODC devotes particular attention is that of capacity-building in the area of international cooperation to combat cybercrime. Apart from its legislative assistance, and in an effort to help practitioners to draft effective and accurate MLA requests, to receive more useful responses and to streamline the relevant process, UNODC has developed a Mutual Legal Assistance Request Writer Tool (MLA Tool), which can be used for all serious offences and not just those covered by international conventions.[13]

Since the Seventh Session of the Conference of the Parties to the UN Convention against Transnational Organized Crime (October 2014), UNODC has been working intensively to revise and update the MLA Tool. The redeveloped content and structure of the tool were finalized in May 2016, thus enabling the launching of a pilot phase to test its use in practice. Currently, the Tool is available in English, French, Spanish, Russian, Portuguese, Bosnian, Croatian, Montenegrin and Serbian.[14] The first countries where the redeveloped Tool was tested were Ethiopia, Uganda and Kenya in July 2016. The findings of the pilot testing were brought to the attention of the Conference of the Parties to the UN Convention against Transnational Organized Crime at its Eighth Session in October 2016.

The new guiding elements in the revised text of the MLA Tool include an additional "digital evidence module". That module takes into account all pertinent developments in the field of international cooperation to combat cybercrime, and covers the following forms of cooperation: (a) expedited preservation of stored computer data; (b) ensuring access to stored computer data; and (c) real-time collection of traffic data.

Several international and regional organizations, including the COMSEC, ITU, UNCITRAL, UNCTAD, UNODC and the CoE provide assistance to countries and regions. These agencies are increasingly joining forces to maximize the impact of their actions (*see* box 6.1, below).

Box 6.1: UNCTAD Assistance to Partners[15]

In support of developing countries' efforts in this area, UNCTAD assists in the preparation and revision of e-commerce laws aligned with international and regional instruments. In the past decade, over 2,500 policy and law makers were trained in the ASEAN, EAC, ECOWAS, Latin America and the Caribbean. The assistance provided by UNCTAD has created a stimulus for countries to push for the adoption of national laws in this area. The work has involved close collaboration with regional institutions such as the AU Commission, the ASEAN Secretariat, the EAC Secretariat, the ECOWAS Commission, the *Asociación Latinoamericana de Integración* (ALADI) and the *Secretaría Permanente del Sistema Económico Latinoamericano y del Caribe* (SELA).

Over sixty countries have been engaged with UNCTAD thanks to the financial support of Finland and Spain. Capacity-building activities have strengthened the knowledge of policy and lawmakers with regards to the legal issues surrounding e-commerce and international best practices, allowing them to formulate laws that correlate with their regional frameworks.

Several agencies are assisting developing countries within their mandates, and inter-agency collaboration is growing. An example is the jointly organized briefing of Commonwealth parliamentarians by UNCTAD, the CTO and the Commonwealth Parliamentary Association during the Commonwealth Cybersecurity Forum in 2013. Another example is the joint workshop on the harmonization of cyber legislation in ECOWAS that took place in Ghana in March 2014. The event was organized by UNCTAD, UNCITRAL, the African Centre for Cyberlaw and Cybercrime Prevention, CoE, and CCI.

UNCTAD has built a network of institutions with which it regularly partners with on different projects and activities. Many of them contributed to the development of the Cyberlaw Tracker database, which maps laws in the areas of e-transactions, data protection, cybercrime and the protection of consumers online. The results of this first-ever global mapping are available online.[16]

C. Knowledge Sharing & Dissemination

Knowledge sharing and dissemination can take place through both training workshops and through formal and informal networking among participants at the national and regional levels. Regardless of the approach, it is important to promote beneficiary involvement to ensure sustainability and ownership, and to tailor the training session depending on the needs of the various stakeholders.

Regional and national capacity-building activity should aim to:

- Raise awareness of cybercrime issues among policy makers and other stakeholders;

- Exchange good practices among participants from other countries and from regional and international organizations;
- Discuss possible regional coordination; and
- Set the stage for further assistance and action.

An effective way to approach capacity-building is to combine distance-learning with face-to-face training workshops. Doing so allows for a flexible training process that includes active participation.

Distance learning allows trainees to:

- Choose the time and place of learning that suits them best;
- Exchange information and ideas with trainers and fellow trainees regardless of location;
- Benefit from continued partner support, such as that offered by the UNCTAD TrainForTrade team (discussed below); and
- Maintain contact with international trade specialists and other training institutions.

Some international organizations, such as UNCTAD, are using models that include distance learning trainings followed by face-to-face workshops at the national and regional level (*see* box 6.2, below).

The UNODC Global eLearning Programme is designed to offer on-demand capacity-building to stakeholders around the globe on contents related to UNODC staff. The tailored training courses are developed by UNODC in collaboration with international experts and correspond directly to needs of Member States. They are comprised of different subjects, including cybercrime.[17]

Box 6.2: UNCTAD TrainForTrade Learning Methods[18]

Combining distance and face-to face learning: UNCTAD's TrainForTrade Programme combines face-to-face activities with distance-learning courses. Experience shows that the quality of face-to-face seminars increases (in terms of trainees' participation and learning results) when trainees have first been introduced to the relevant subject matter through an e-learning course. TrainForTrade emphasizes that the pedagogic aspects of training should not be undermined by technology. At the same time, the use of ICT as a tool for knowledge-sharing increases the number of beneficiaries, while also keepings the costs down. Experience shows that adult trainees typically learn better in a group environment. Consequently, TrainForTrade courses use chat rooms and group foraums to facilitate exchange with the instructors and amongst participants.

Training the local distance-learning tutor: One essential element of TrainForTrade includes training local experts as tutors to moderate and locally manage the distance learning deliveries. The identification of a training center and a local tutor is essential for maximizing

the impact of the course. During the training of technical tutor's course, a local tutor learns the process of course delivery and the different pedagogic strategies that he should use to facilitate the delivery.

Meeting the needs of beneficiaries: The choice of training methods and technology will always depend on the characteristics and circumstances in the beneficiary country. TrainForTrade uses Moodle, a free and open-source learning management system based on a Linux platform in order to facilitate the sharing of information and technology in an efficient and cost-effective manner.

Continuous evolution and development: TrainForTrade is continuously developing new learning tools by exploring new technological opportunities. The expansion of 3G/4G coverage, cell phones, smartphones and tablets has made access to information easier. The development of cloud and mobile learning provides efficient solutions for the storage, dissemination and acquisition of information. The tools can also be used to promote interactive and collaborative learning.

Another important way to create awareness is to promote information-security awareness in the population at large. Individuals and enterprises—especially SMEs—increasingly need to be made aware of not only the relevant and ever-changing laws, but also of their rights. Doing so is particularly important in order to build trust in cross-border e-commerce. Industry associations and consumer protection agencies should work together to overcome barriers caused by divergent national legal standards. National public campaigns (including through radio and television programs) aimed at informing about ways to protect consumers online can be a key element of awareness-raising strategies (*see* box 6.3, below).

Box 6.3: Awareness Campaigns on e-Commerce Laws in Uganda[19]

In Uganda, the National Information Technology Authority (NITA)[20] and the Ministry of Information and Communications Technology[21] developed and facilitated the enactment of subsidiary legislation to operationalize the EAC Framework on Cyber Laws (UNCTAD, 2012).[22] Since 2011, NITA has embarked on a campaign meant to raise awareness about new laws, as well as aspects of information security in general.[23] The campaign aims to encourage public administration and private sector actors to put minimum information security controls in place in order to ensure safe e-transactions. Sensitization workshops have been organized for entities such as ministries, banker association, and legal societies, as well as for national chambers of commerce, the Investment Authority and the Securities Exchange. Workshops have been facilitated by a multi-institutional team of lawyers and technical resource persons,

including experts participating in the EAC Task Force supported by UNCTAD. Future plans include the delivery of similar workshops to create awareness of the Data Protection and Privacy Bill, once enacted.

Conclusion

Building capacity and raising awareness about combatting cybercrime should be a national priority for every country. To address cybercrime at the national level, domestic legal frameworks must be developed. Countries must also coordinate and cooperate across borders with governments and agencies in the formulation of their cybersecurity strategy. Coordination and cooperation is necessary to ensure a shared minimum understanding and interoperability of competencies internationally, on both procedural and substantive levels. However, there remain many challenges, which must be faced. These include, among others, resources and funding, understanding the fast-evolving nature of cybercrime, the slow pace of elaborating legislation, enforcements issues and the implementation of effective regimes to combat cybercrime.

One of the key issues in fighting these challenges is making sure that policy makers, law makers and law enforcement receive adequate training on combating cybercrime. Dissemination and sharing of knowledge that takes place during these training sessions benefits the cybercrime awareness of a country. International organizations, such as UNCTAD, help with the training of local staff (*e.g.*, via UNCTAD's TrainForTrade). Another way to improve awareness is by promoting cybersecurity issues within the population in general, as was done in Uganda, for example. Furthermore, to support national capacity-building, multilateral and bilateral agencies might help by assisting in the preparation and revision of a range of cyberlaw approaches in order to align them with international and regional good practices. By cooperating and coordinating both at the national as well as the international level, these methods help raise awareness of cybercrime and help build cybersecurity capacity.

Annex

Global Cybersecurity Index 2017 – Good Practices

Country	Good Practices
Mauritius	The top-ranked country in the Africa region, Mauritis scores particularly high in the legal and the technical areas. The Botnet Tracking and Detection project allows Computer Emergency Response Team of Mauritius (CERT-MU) to proactively take measures to curtail threats on different networks within the country. Capacity-building is another area where Mauritius does well. The government IT Security Unit has conducted 180 awareness sessions for some 2,000 civil servants in 32 government ministries and departments.
USA	With the highest scores for the legal and capacity-building pillars, one notable aspect of both capacity-building and cooperation in the country is the initiatives to coordinate cybersecurity among all states. To that end, the National Governor's Association established the Resource Center for State Cybersecurity, which offers best practices, tools and guidelines.
Egypt	Ranking second with a full-range of cooperation initiatives, Egypt is a member of the UN Government Group of Experts (GGE) on cybersecurity, has chaired the ITU Working Group for Child Online Protection, was a founding member of AfricaCERT and has a number of bilateral and multilateral agreements on cybersecurity cooperation.
Malaysia	Ranked second in the Asia-Pacific region and scores a perfect 100 on capacity-building, Malaysia has developed a range of initiatives in that pillar. Notably, Cybersecurity Malaysia, the government entity responsible for information security in the country, offers professional training via higher education institutions in Malaysia. It maintains the Cyberguru website, dedicated to professional security training.
Georgia	Top-ranked in the CIS, the government has strongly supported protection of Georgia's information systems after large-scale cyberattacks on the country in 2008. The Information Security Law established a Cyber Security Bureau with a particular emphasis on protecting critical information systems in the military sphere.
Estonia	The highest ranked nation in the Europe region, Estonia, like Georgia, substantially enhanced its cybersecurity commitment after a 2007 attack. This enhancement included the introduction of an organizational structure that can respond quickly to attacks as well as a legal act that requires all vital services to maintain a minimal level of operation if they are cut off from the Internet. The country also hosts the headquarters of the NATO Cooperative Cyber Defence Centre of Excellence.

B. Developing Capacity-building Programs

Table of Contents

Introduction

As discussed, capacity building starts by creating the framework and infrastructure that allows for capacity to build and to be built; that involves developing an overarching cybersecurity policy and strategy (*see* section 2 F, above), passing the necessary cybercrime-specific legislation (*see* section 3 A, above) and creating specialized cybercrime units (*see* section 1 D, above). Only thereafter can targeted cybercrime capacity-building programs be launched. While the area is a still developing, a multitude of approaches to training techniques exist, as offered by a multitude of organizations.[1] Those programs may **(I)** offer cybercrime training for government authorities, with different courses targeted for law enforcement personnel and members of the prosecutorial and judicial services, respectively. Whichever approach is taken, **(II)**

cybercrime capacity-building programs must be client-driven if they are to be effective, meaning that, while donor and partners might well bring their own interests and expertise, the program must be client-owned for the program to be truly efficacious. In order to elucidate all of these aspects, this section concludes by **(III)** exploring the CoE's experience with capacity-building programs by considering the Budapest Convention and by looking at several project examples.

I. Offering Cybercrime Training for Government Authorities

While creating units specialized in the handling of cybercriminal matters is important, it is equally important to offer training in foundational cybercriminal matters—including institutional structure and resource availabilty—both **(1)** to law enforcement personnel and **(2)** to members of the prosecutorial and judicial services. In order to be truly effective, such trainings should be sustainable, standardized, replicable and scalable.

A. Training for Lawmakers

As the Toolkit has attempted to make evident, the fight against cybercrime begins with the construction of legal frameworks that are not only robust in their own right, but, due to the internet's global nature, which are interoperable with the legal frameworks of other nations (*see* section 1 B, above). As lawmakers are chiefly responsible for the development of such frameworks, they play an essential role in the success of any long-term capacity-building programs. To that end, lawmakers ought to be made knowledgeable about the nature of cybercrime at large and about the policies and laws of other nations.[2] In addition to paying detailed attention to targeted sectors, such as the financial sector, lawmakers must be both aware of, and willing to work with, the webbed, intertwined interactions between international instruments and various domestic laws. Further, law makers need the background to be able to foresee economic, constitutional and social impacts of the cybercrime legislation and policies that they develop.

B. Training for Law Enforcement Personnel

Beyond the creation of specialized units discussed above, and in addition to creating strategic structures and connections for general knowledge dissemination and discussion, foundational cybercrime training should be offered to those on the frontlines of dealing with cybercrime. Indeed, many countries already provide training on general mechanisms via courses or through on-the-job exposure.

Training is important as all types of crimes increasingly involve or implicate cyberspace, be it in the form of electronic evidence, or through the use of ICT. As any law enforcement officer, prosecutor or judge inevitably will be confronted with such matters, they should be appropriately prepared for, and familiarized with, such matters.

Comprehensive cybercrime training to authorities should include the following areas:

1. **Investigating cybercrime.** As discussed (*see* sections 2 C & 2 D, above), investigating cybercrime requires different skills than those typically used to investigate traditional crimes. In particular, awareness should be raised about procedural differences, methods of ICT forensic analyses and techniques for preserving the authenticity, integrity and reliability of electronic evidence. Understanding existing law enforcement training materials and initiatives might help elucidate this process.[3]

2. **Differentiating functions.** In addition to understanding how the larger system operates, it is also important for stakeholders and actors to understand the skills and competencies, as well as functions at appropriate level, of respective units (from first responder to forensic investigators). Methods of offering inter-agency cross-support, while also assuring network security should all be covered.

3. **Facilitating cooperation.** For fighting crime in general, it is important that the various authorities cooperate; such is especially the case in cybercrime, where evidence can be nearly ephemeral and may be divided and stored in numerous countries. Cooperation for training purposes should foremostly focus on creating connections between public authorities (law enforcement, prosecutors, judiciary) but should also extend to including ways of working with academia and industry.

C. Training for Prosecutors & Judicial Authorities

Foundational cybercrime training is not only important for law enforcement officers, who are the first to come into contact with such evidence, but also should be offered to authorities at all levels—investigatory, prosecutorial and judicial authorities alike. Indeed, while specialized cybercrime units are most typically found among police services (where discrete technical support is frequently required), such units are very infrequently found in prosecutorial services and (even less so) in the judiciary. As such specialized services are not always available to prosecutors and judges, foundational cybercrime training is particularly important for these professionals. However, and notwithstanding this need, training on cybercrime and electronic evidence is very rarely offered on any basis, let alone regularly, to prosecutors or judges. Lack of knowledge and skills among prosecutors and judges persists as a point of concern around the world, regardless of the country or region.

While trainings may be held in common—and, indeed, should in part be held in common—it is advisable for trainings to be targeted and audience-specific, especially in light of the division of powers between investigators/prosecutors and the judiciary.[4]

Thus, in addition to exposing prosecutors and judicial authorities to the training offered to law enforcement authorities (as discussed immediately above), training programs tailored to the needs of prosecutors and judicial authorities should address the following matters:

1. **Cybercrime basics.** The course should present an understanding not only of the nature of cybercrime, but also of cyber how cybercrime is addressed by law enforcement authorities. Attention should be given to (a) adapting training materials to the needs of the jurisdiction where the training is being offered, (b) to tailoring the training of trainers and (c) the mainstreaming of these cybercrime modules into regular training curricula.

2. **Advanced training.** The matter and material for cybercrime being copious, separate modules should be offered for more advanced and nuanced topics, including specialization and technical training.

3. **Networking.** Enhanced knowledge might be accomplished through the networking of judges and prosecutors, and regularly making caselaw and other resources available.[5]

D. Knowledge Sharing

All states and institutions face difficulties in curating and disseminating knowledge. While creating special cyber units and cooperation mechanisms is important, standardized training, on-the-job training and *ad hoc* courses or informational bulletins for authorities at all levels can all be used to facilitate and further the process. It is important that knowledge be shared as broadly and as routinely as possible.

Additionally, care should be taken to assure that dissemination is done geographically—for instance, a cyber unit may be located in the capital city, but, due to the nature of cybercrime, significant cases will almost certainly occur elsewhere in the country. As such, it is also necessary to target knowledge sharing by profession—for example, judges should be aware of matters such as instances when foreign electronic evidence may be properly admissible, even if informally procured by police.

Although the creation of specialized cyber units and the offering of targeted trainings may imply the importance of knowledge, the critical nature of such activities merits flagging such measures here under a separate heading. Additionally, it bears noting that many officials in many governments are hesitant to embrace electronic evidence—or e-evidence—, or they may be reluctant to accept

training on the topic for various reasons, including that they are already experts in one field and do not care or need to be trained in another. Such resistance impedes the acceptance of electronic evidence and international cooperation; with that in mind, consciousness-raising and training should be tailored accordingly tailored. Routine knowledge sharing mechanisms can help mitigate such mistrust or discomfort.[6] Relatedly, participation in international conferences and sharing exercises with homologues of other nations can contribute significantly: the effects of informal and personal connections, especially as when encouraged alongside formal arrangements and structures, ought not to be underestimated (*see* section 5 B, above).

E. Furthering Public-Private Cooperation

Cooperation and information exchange are essential to effectively combatting cybercrime. Such is especially the case as so much of the infrastructure that is essential to the functioning and "existence" of cyberspace is owned, controlled or operated by the private sector as opposed to the public sector. ISPs, financial sector institutions and other industry actors are all essential to the effort to combat cybercrime. To that end, initiatives, including CERTs, CSIRTs, academic and non-governmental projects have been launched.

Any such program should seek to do the following:

1. Strengthen cooperation between law enforcement and private sector operators;
2. Support the creation of Information Sharing and Analysis Centers (ISACs), especially for the financial sector;
3. Set-up of cybercrime reporting systems (such as for spam, botnets, child abuse materials);
4. Facilitate cooperation between law enforcement and CIRTS, CERTs or CSIRTs; and
5. Further private-public information sharing in line with data protection requirements.[7]

F. Advancing International Cooperation

Cyberspace is transnational by nature. As such, e-evidence of a cybercrime is quite frequently scattered around jurisdictions, and, indeed, around the world at large. As such, investigators need to be able to secure electronic evidence which, in part, piece or whole, might be beyond the place of their own jurisdictional authority, often with great speed. To that end, international efforts should be undertaken to train and support competent authorities to engage in efficient and expedited international cooperation. Such programs should not only familiarize members of government with the resources in their own jurisdictions, but connect them with their counterparts—domestically, regionally and internationally.

Such programs should focus on the following:

1. Strengthening domestic activities as a basis for international judicial and police-to-police cooperation;
2. Setting up 24/7 points of contact for urgent international cooperation, in particular data preservation;
3. Training and networking of authorities for MLA; and
4. Ratification of, or accession to, international treaties and conclusion of bilateral agreements.[8]

II. Client-driven Capacity Building

Although there may be many ways to sequence activities, capacity-building programs should be developed and implemented in a pragmatic manner that aligns with the needs of the target group—that is, the client. Therefore, a program should support the government, agency or organization seeking to change. The request for assistance should come from that entity, and that request should structure the way in which the assistance is to be provided. Assistance should not be donor driven.

Generally speaking, strengthening legislation on cybercrime and electronic evidence is a suitable starting point to enter into dialog. By contrast, starting a program with computer forensic training courses, for example, without having developed a legal framework on cybercrime may prove to be of limited use.

Experience shows that engagement of decision-makers is essential for the success of capacity-building programs and for advancing any substantial criminal justice measures in cybercrime in general. A thorough analysis of the cybercrime situation and of the strengths and weakness of criminal justice capabilities will facilitate the engagement of decision makers and will establish benchmarks against which progress can be determined later on.

Towards the end of a program (or of a phase thereof), an assessment of the progress made should be undertaken. Thereafter, for that assessment to be of effect, feedback mechanisms should relate back to the overall policies and strategies, seeking to reconfirm the engagement of decision-makers beyond the completion of the program.[9]

III. Capacity-building Programs: The CoE's Experience

Of the great diversity of cybercrime capacity-building programs that exist, the CoE has had extensive experience, largely structured around **(A)** implementing the Budapest Convention, as well as through **(B)** a variety of cybercrime capacity-building projects, be they country-specific, regional or global.

A. Implementing the Budapest Convention

The CoE approach on cybercrime consists of three interrelated elements:

1. Setting common standards;
2. Following-up and assessing implementation; and
3. Providing technical assisstance that furthers cooperation for capacity building.[10]

The Council's standards are fundamentally drawn from the Budapest Convention, and its Additional Protocol on Xenophobia and Racism committed by means of computer systems. Additional standards come from the treaties on data protection (Convention 108)[11], on the sexual exploitation and sexual abuse of children (Lanzarote Convention),[12] on money laundering and financing of terrorism[13] and others. The key supervising body is the Cybercrime Convention Committee (T-CY), which not only represents the Parties to the Budapest Convention ("Consultations of the Parties"), but also interprets the text of the Convention, prepares Guidance Notes and assesses the Parties' implementation of the Convention.[14]

The Council's approach to capacity building is aimed at assisting governments and organizations in the implementation of the Budapest Convention and related standards, including human rights and rule of law principles and in following up on the assessments carried out by the T-CY. In a dynamic circle, results of capacity building in turn inform standard-setting and the larger work of the T-CY.

B. CoE Cybercrime Capacity-building Projects

Since 2006, CoE has carried out a range of country-specific, regional and global capacity-building projects. Additional projects are in preparation. Many projects are co-funded by the European Union. The EU supports the Budapest Convention and capacity building on cybercrime worldwide. These include: **(1)** Global Action on Cybercrime (GLACY), **(2)** Global Action on Cybercrime Extended (GLACY+), **(3)** Cybercrime@Octopus, **(4)** Cybercrime@EaP II, **(5)** Cybercrime@EaP III, **(6)** iPROCEEDS and **(7)** C-PROC.

1. Global Action on Cybercrime (GLACY)

The Global action on Cybercrime, or GLACY, was a joint project of the EU and the CoE aimed at supporting countries worldwide in the implementation of the Budapest Convention.[15] The specific objective of GLACY was "to enable criminal justice authorities to engage in international cooperation on cybercrime and electronic evidence on the basis of the Budapest Convention on Cybercrime". The project's duration was three years, from 1 November 2013 to 31 October 2016.

GLACY was intended to explore measures that would:

1. Engage decision-makers;
2. Facilitate the harmonization of legislation;
3. Develop judicial training programs;
4. Expand the capacities of law enforcement;
5. Improve international cooperation;
6. Increase information sharing; and
7. Assessment of progress.

2. Global Action on Cybercrime Extended (GLACY+)

Building upon the success of GLACY,[16] the CoE and the EU's Instrument Contributing to Peace and Stability launched Global Action on Cybercrime Extended, or GLACY+, which runs from 1 March 2016 until 28 February 2020. Intended to extend the experience of the GLACY project, GLACY+, though a global action, initially supports nine priority countries in Africa, the Asia-Pacific region and Latin America, namely: the Dominican Republic, Ghana, Mauritius, Morocco, Senegal, South Africa, Sri Lanka and Tonga. These countries are intended to serve as hubs for knowledge and experience sharing for their respective regions. The objectives of GLACY+ include strengthening the capacities of States around the world through the development and application of cybercrime legislation, while also enhancing their abilities for effective international cooperation in this area.

More general objectives for GLACY+ include the following:

1. Promoting consistent cybercrime and cybersecurity policies and strategies;
2. Strengthening the capacity of police authorities to investigate cybercrime and engage in effective police-to-police cooperation with each other as well as with cybercrime units in Europe and other regions; and
3. Enabling criminal justice authorities to apply legislation and prosecute and adjudicate cases of cybercrime and electronic evidence and engage in international cooperation.

3. Cybercrime@Octopus

Cybercrime@Octopus is a CoE project based on voluntary contributions that aims at assisting countries around the world in how best to implement the Budapest Convention and to strengthen data protection and rule of law safeguards at large.[17] The project had a three-year duration, from 1 January 2014 to 31 December 2017.

The results of Cybercrime@Octopus include the following:

1. Annual Octopus conferences, with attendees from around the globe;
2. Co-funding and supporting the T-CY; and
3. Providing advice and other assistance to states prepared to implement the Budapest Convention and related instruments pertaining to data protection and the protection of children.

4. Cybercrime@EaP II

A partnership jointly implemented by the EU and the CoE's Programmatic Cooperation Framework in the Eastern Partnership (EaP) Countries, Cybercrime@EaP II aims to optimize the regional and international cooperation on cybercrime and electronic evidence.[18] Participating countries are the six EaP countries: Armenia, Azerbaijan, Belarus, Georgia, Moldova and Ukraine.[19] The project runs from 1 May 2015 to 31 October 2017. Specifically, the project aims to improve of MLA in matters of cybercrime and electronic evidence, and strengthening of the role of 24/7 contact points.

5. Cybercrime@EaP III

With a similar timeframe as Cybercrime@EaP II (1 December 2015 to 31 December 2017), and similarly implemented by the EU and the CoE's Programmatic Cooperation Framework in the EaP countries, Cybercrime@EaP III is a complementary capacity-building program.

Cybercrime@EaP III aims at improving cooperation between criminal justice authorities and service providers in specific criminal investigations, while also upholding necessary rule of law safeguards.[20] As with Cybercrime@EaP II, participating countries are the six EaP.[21]

6. Cooperation on Cybercrime under the Instrument of Pre-accession (iPROCEEDS)

Targeting eastern Europe and Turkey, Cooperation on Cybercrime under the Instrument of Pre-accession (IPA), or iPROCEEDS, is a joint project of the EU's IPA II Multi-country action program 2014 and CoE. Its objectives are to strengthen the capacity of authorities in the IPA region to search, seize and confiscate cybercrime proceeds and prevent money laundering on the internet. Project indicators include the extent of financial investigations and prosecutions related to cybercrime and proceeds from online crime, and the level of compliance with international standards on cybercrime, money laundering and the search, seizure and confiscation of proceeds from crime (CoE Conventions 185 and 198). It has a duration period from 1 January 2016 to 30 June 2019, and is being implemented in Albania, Bosnia and Herzegovina, Montenegro, Serbia, the Former Yugoslav Republic of Macedonia, Turkey and Kosovo.[22]

7. Cybercrime Programme Office (C-PROC)

With increasing demand for capacity building on cybercrime and electronic evidence, organizations providing support need to enhance their own capabilities.[23] To that end, and further to an offer by the Prime Minister of Romania, CoE established a Cybercrime Programme Office (C-PROC) in Bucharest, Romania, in 2013. C-PROC is responsible for the implementation of the capacity-building projects of CoE on cybercrime and electronic evidence worldwide. The added value includes specialization, cost-effective project management, competitiveness and thus increased resource mobilization. The activities managed by C-PROC are closely linked to the work of the T-CY and other intergovernmental activities of CoE in Strasbourg, France.

Conclusion

Cybercrime capacity building offers a number of advantages. It responds to needs and produces immediate impact. It favors multi-stakeholder cooperation, as well as contributing to human resources development, poverty reduction and respect for the rule of law, while also reducing the digital divide.[24] Moreover, policy discussions at the international levels show that cybercrime capacity-building programs have broad political support upon which to build. Experience, good practices and success stories are readily available, offering adaptable and replicable results.

Elements of capacity-building programs may include support to cybercrime policies and strategies, legislation including rule of law safeguards; reporting systems and prevention; specialized units, law enforcement and judicial training; interagency cooperation; public/private cooperation; international cooperation; protection of children; and financial investigations. An effective criminal justice response is an essential component of a governance framework that is to ensure the security, confidence and trust in ICT so that societies are able to exploit the benefits of ICTs for development. Strengthening safeguards on law enforcement powers and implementing frameworks for the protection of personal data are an essential precursor to building cybercrime-fighting capacity.

The impact of cybercrime capacity-building programs is diverse and important, substantially not just cybercrime-fighting measures, but also positively impacting the larger fight against crime. Results range from increased use of electronic evidence in criminal proceedings; increased numbers of investigations, prosecutions and adjudications; shorter response times to requests for MLA; more efficient police-to-police cooperation; and other verifiable indicators. More generally, the success of such programs can also be seen in further human development and improved democratic governance.

C. Private Sector Cooperation

Table of Contents

Introduction

The internet and digitization has facilitated commerce, fueled growth and improved the lives of many. Indeed, it has done so to such an extent that it has become central—even critical—to the way that both individuals and society function. The impact of the cyber revolution range from the most basic transactions, to information gathering and sharing, to complex commercial interactions. Moreover, the internet and digitization has become central to the basic operating of critical infrastructure. However, unlike other structure and implements essential to allowing society's function, the vast majority of the infrastructure underlying and undergirding cyberspace is not in public hands but in private ones.

Because so much of the infrastructure and services behind the internet is owned and operated by the private sector, it is essential that the public and private sectors collaborate to both secure that infrastructure and to allow society to continue to develop to the benefit of all. Consequently, cybersecurity is a matter of public safety that can and must be addressed through public-private

cooperation. Even where cooperation already exists, there is room to improve and enhance cooperation between governments and the private sector on cyber security.[1]

In discussing private sector cooperation with government, specific discussion is needed around **(I)** building PPPs and **(II)** some of the notable existing barriers to effective cooperation, with an understanding of good practices made possible through **(III)** the discussion of various examples of existing PPPs designed to combat cybercrime.

I. Building Public-Private Partnerships

In order to build effective PPPs, it is important to **(A)** recall the place of formal and informal international cooperation, before going on to **(B)** outline the scope of PPPs at large and to **(C)** explore the role in the ICT sector partners in particular. Additionally, the **(D)** caveat of tailoring government interventions and **(E)** the need for information sharing ought also to be highlighted.

A. Formal & Informal International Cooperation

As discussed earlier in the Toolkit (*see* sections 5 A and 5 B, above), international cooperation comprises both formal (*e.g.,* mutual legal assistance, extradition, mutual recognition of foreign judgments) and informal mechanisms (*e.g.,* direct police-to-police, 24/7 networks, information sharing and coordination centers).

Both formal and informal mechanisms of international cooperation need to take account of the role of private sector actors. For instance, formal instruments have notable shortcomings regarding cross-border access to data owing to a focus on the matter of provider consent, as coupled with a presumed knowledge of the location of the data in question. Such shortcomings have resulted in increased resorting to mechanisms of informal cooperation.[2]

PPPs are created either informally, through casual agreements or understandings, or formally, by establishing legal arrangements. Collaboration focuses on facilitating the exchange of information on threats and trends, but also for preventing case-specific activities and actions. Such actions complement those of law enforcement and can help mitigate damage to victims.

The private sector does not just speak to industry. Academic institutions play a variety of roles in preventing cybercrime, including through delivery of education and training to professionals, law and policy development and work on technical standards and solutions development. Universities house and facilitate cybercrime experts, even hosting CIRTs and other specialized research centers.[3] CIRTs play an important role in capacity-building through event-hosting and information sharing, very frequently at a technical level. They also facilitate interactions with local police for identifying cybercriminals, offer important support to the private sector for supporting and coordinating with

other CIRTs to exchange real-time technical data and technical expertise for tracking cybercrimes. These networks extend to regional groups, such as APCERT in the Asia-Pacific region[4] and OIC-CERT for the Organisation of the Islamic Cooperation,[5] and international groups, such as Forum of Incident Response and Security Teams (FIRST).[6] The activities undertaken by these groups are supported through international efforts, such as ITU's regionally-supported ALERT cyberdrills, which involves the host country, ITU, FIRST and privatesector actors.[7]

B. The Place for the Private Sector at Large

As so much of the relevant infrastructure is in the hands of the private sector, and as cyber has infiltrated virtually every domain of life, PPPs are essential to successfully combatting cybercrime. Indeed, INTERPOL has noted that "the complex and ever-changing nature of the cyberthreat landscape requires high-level technical expertise, and it is essential that law enforcement collaborates across sectors to effectively combat cybercrime and enhance digital security."[8] Presently, law enforcement faces many challenges in scaling-up to address the ever-growing threats emanating from cyberspace.[9]

> **"The internet of things presents unprecedented opportunities for criminals, and for effective law enforcement getting perpetrators behind bars should be an integral part of any strategy. Combating cybercrime requires a unified approach, not just in developing partnerships but in ensuring that police around the world are provided with the basic equipment and training they need."[10]**

As already discussed, the so-called internet of everything (IoE) sets to dramatically expand the present understanding of what makes the "infrastructure" of information society, and, correspondingly, to increase criminal opportunities (*see* section 2 A, above). However, such partnerships have heretofore been, as the US White House remarked, "at best unclear or ill-defined" with any detailed allocation of roles and responsibilities between industry and government being left unaddressed.[11]

The development of NCSs, though perhaps structured by the government, must create a space for the private sector as an essential part of combatting cybercrime. This realization is a shared responsibility requiring coordinated action related to the prevention, preparation, response and recovery from incidents by all stakeholders—government, the private sector and civil society at large.[12]

Use of a PPP-approach is not without criticism.[13] Published NCSs typically approach critical infrastructure protection from the perspective of a common-good, with all actors supposedly working in harmony to achieve a common goal.[14] Attempts to enhance the dialogue between the public and private sectors often have been unsatisfactory due to issues such as lack of

trust, misplaced expectations, conflicts of interest and laws requiring a certain level of secrecy or openness that may work against the interest of the private actor in question. Further, in a recessionary economy, with industry tending to focus on short-term delivery of revenue lines for survival, longer-term strategic issues may be relegated to secondary importance. Matters such as the stand-off between the FBI and Apple, and the indications of government usage of telecommunications to improve surveillance, for instance, have done little to improve working relations between the two sectors (*see* section 1 B, case 1.3, above).

Box 6.4: Academic and Government PPPs[15]

Academia plays an important role in building effective PPPs. For instance, the National University of the Philippines and the US DoJ signed an agreement in 2012 for a PPP to develop cybercrime experts through Southeast Asia's first four-year course on digital forensics. The course—a Bachelor of Science in Computer Studies, Major in Digital Forensics—is intended to develop professionals in the specialized field, particularly in the area of evidence retrieval from computer hard disks, mobile phones and other ICT devices. The long-term PPP is intended to provide institutionalized capacity-building and to allow resource sharing in order to face the global challenge of cybercrime by mobilizing subsequent generations.

C. Involving ICT-Sector Players

While PPPs at large can be beneficial, there is a particular need to create partnerships involving ICT sector players. ICTs continue to develop and to be diffused at an incredible pace, dramatically changing the way in which societies operate, and driving near unprecedented economic and social development.[16] As such, private entities operating in the ICT sector—the drivers of much that progress—are particularly important for developing crime-solving PPPs. Additionally, private sector actors are often better poised to play a constructive role: first, they frequently have greater control over many of the critical systems in need of protection and of relevant data; second, they often have more resources than government for recruiting top talent; and, third, they typically do not face many of the constitutional and statutory limitations that control government's investigations and police powers.

Moreover, the contributory role that ICT entities could play is not merely benevolent: as so much about market success is consumer confidence, ICT entities have many commercial reasons for investing strongly in promoting a safe and secure cyberspace at large, both in their own research and innovation (R&I), as well as in cooperating with the public sector. Given the substantial private R&I being undertaken, ICT companies have an array of security tools that could support public efforts to fight cybercrime.

D. Tailoring Government Interventions

While the private sector has crucial insight, expertise and resources for combatting cyberthreats, the government is uniquely positioned to investigate, arrest and prosecute cybercriminals; to collect foreign information on cyberthreats; and, potentially, to provide certain statutory protections to companies that sharing information with government,[17] much as is done for whistleblowers in anticorruption efforts. Government also may be privy to threat information—from both domestic and foreign sources—in advance of the private sector and can collect and disseminate information among the various and diverse stakeholders. Government can provide a more complete perspective on the threat and on effective mitigation techniques, while taking steps to protect individual victims. This can help assuage competitive and reputational concerns about revealing a particular company's vulnerabilities to its competitors, the marketplace and cybercriminals.

Moreover, even where critical systems are owned and operated by private companies, the public's expectation is often still for government to ensure the security and integrity of those systems, and to respond when damaged or otherwise compromised. As such, it is generally in the interest private sector actors to partner with government so that, when necessary, government interventions are efficacious, limiting counter-productivity or heavy-handedness.

E. The Need for Information Sharing

Though important in any area, robust information sharing and cooperation between the public and the private sectors is particularly important—and notably absent—with regard to cybercrime, largely due to differences in the nature, type and access to pertinent information and capabilities of the two sectors. For instance, having reporting mechanisms for hacked companies to promptly report breaches and allow government access to identify points of entry and other vulnerabilities, or for banks and credit card companies to rapidly identify and track compromised data and provide credit card numbers that are active but not tied to actual identities and to identify and track activity of compromised cards and illicit payments.

As discussed earlier (*see* section 1 C, case 1.5, above), when Albert Gonzalez stole more than 130 million credit card numbers, it was determined—after the fact—that the attacks were connected and likely from the same source.[18] Specifically, the government determined that the same code appeared in the SQLi strings that were used to gain backdoor-access to the victims' systems, and that the infiltration IP address (for injecting malicious code into those systems) and exfiltration IP address (for receiving the credit card data that was removed from the systems) were the same for each incident.[19]

Cybersecurity coordination is too often episodic or bureaucratic. Across initiatives, a workable culture of information sharing and coordination needs to be implemented. Appropriate institutions must be created to effectuate the implementation of these cultural shifts, as many private actors

still do not know whether, when or how it would be beneficial (or detrimental) to engage with government on these issues. Moreover, as the legal landscape is evolving, it is important that government and private sector communicate regarding the appropriate roles and capabilities, and that authorities in law enforcement agencies and regulatory agencies make clear potential sources of civil liability.

II. Barriers to Effective Cooperation

Despite its importance and the potentially significant impact of a campaign to harmonize the efforts of the government and private sector in cybersecurity, there exist many legal, pragmatic, cultural and competitive barriers to effective cooperation.[20]

Several of the more important reasons follow:

1. **The lack of prophylactic cooperation:** Despite the pervasive and persistent threat, many companies consider actively working with government once they are faced with responding to a cybersecurity incident and are in crisis mode. It is important to create a mental shift that will facilitate cooperation that occurs in times of relative calm, and which progresses in an ongoing, proactive basis well before a crisis occurs and without a cyber incident becoming apparent. Moreover, corporate decision-makers who have not previously dealt with government in a collaborative way may be less keen on doing so when dealing with a cyber-incident and its fallout. By working prophylactically, trust is built early-on, and cooperation—when needed—can be more effective and efficacious.

2. **The problem of appearances of working with government:** Although typically having greater and more strategic resources to bring to bear in the fight against cybercrime, private sector entities may fear collateral consequences of involving the government in cyber-incident responses. Such a reaction is partially due to confidence in their own capabilities to handle such problems. However, there may also be concerns about appearing to be give government access to sensitive user data and the potential for retribution by market forces from such cooperation. Both public and private sector actors are guilty of failing to sufficiently share information.

3. **Stuck in reactivity, not proactivity:** The private sector's comportment has largely been one of reactivity rather than pro-activity. By and large, there has been a general "check-listing" approach in terms of establishing cybersecurity and combatting cyberthreats. In the wider commercial community, acceptance of a shared obligation for security is, as yet, unestablished. There are many reasons for such a perception, not least of which is the competitive nature

of free-market economies, as well as a history of indifference by the private sector, which has traditionally assumed that government will protect them in the event of cyberthreats.[21] Robust and participatory engagement must balance wider business community with investigative force.

4. **Lack of understanding at the individual level:** There is no cohesive effort to integrate either SMEs or individuals into the effort to develop cybersecurity and to build society-wide cyber-resilience. Unlike those working to secure critical infrastructure and creating a shared goal of security, there is hardly any perceived connection between SMEs and individuals to the notion of ownership of building communal cyber-resilience. As such, the disparate consumer audience flounders to find commonalities. Moreover, at the level of the individual consumer, there are—especially in developed nations—reports surfacing of "security fatigue"; such fatigue, it has been found, can cause computer users to feel hopeless and to act recklessly with regard to matters of cybersecurity.[22] The lack of any cohesive cybersecurity understanding means that cyber resilience at the consumer level struggles to even identify those who should be partners, let alone those who would be leaders in such an undertaking.

5. **The problem of a government-centric approach:** Official policy could go further to facilitate and to incentivize private sector involvement. Indeed, according to industry experts, many government-developed cybercrime centers are structured to focus on protecting government systems and critical infrastructure but tend to leave out the private sector. As such, private sector actors, though possibly contributing to the efficacy and functioning of those centers, do not necessarily benefit from such government efforts, therein leaving their computer systems vulnerable to cyberattacks.[23] Moreover, and as already noted, substantial information sharing shortcomings endure.

6. **Concern over lacking safeguards:** Lastly, a general sense of malaise and suspicion limits the willingness of some private sector actors to grant government access. This skepticism is two-fold: on the one hand, there is concern that one government agency might pass along potentially incriminating information to another agency.[24] On the other hand, there is concern that government is spying on the businesses and consumers with which government is trying to engage.[25] Recent reports of government spying have done little to assuage such suspicions and concerns.

III. Examples of Cyber PPPs

Although there are barriers to building PPPs, yet there are some important successes in **(A)** corporate social responsibility, **(B)** combatting online scams and fraud, **(C)** private-sector originating

initiatives, **(D)** inter-governmental and international initiatives, **(E)** initiatives in Europe and **(F)** initiatives in the United States.

A. Corporate Social Responsibility Examples

Examples of effective corporate social responsibility collaboration between crime agencies and ICT companies exist with regard to cybercrime, fraud protection, online safety and security and fighting child exploitation. These models demonstrate not just the value of such collaboration but also the sheer variety in the nature of the response.[26]

B. Combatting Online Scams & Fraud

Collaboration to combat online scams and fraud are rapidly increasing. For instance, more than one hundred governments work with Microsoft in its Security Cooperation Program (SCP)[27]. This program provides protection from critical risks to information and infrastructure and helps to reduce government vulnerability to attacks that can critically disable administration and disrupt economies. A biannual global Security Intelligence Report provides in-depth insight into the threat landscape of the moment based on data derived from hundreds of millions of computers worldwide.[28] On average, seventeen percent of reporting computers worldwide encountered malware over the past four quarters.[29] Further, other high-severity vulnerabilities, such as downloaded Trojans, continue to be on the rise. The aggregated data indicates that financial gain remains attackers' top motivation.

Accounting for divergent motivations has also become an issue. For example, hacktivists and practitioners of military and economic espionage are relatively recent newcomers and have different interests from typical cyberattackers. Additionally, the nature of the attack strategies has changed, with rogue security software or fake antivirus software used to trick people into installing malware and disclosing sensitive information being replaced by ransomware that seeks to extort victims by encrypting their data. Commercial exploit kits now dominate the list of means of compromising unpatched computers, meaning attacks are increasingly professionally managed and constantly optimized at an increasingly rapid rate. Targeted attacks have become the norm rather than the exception.[30]

C. Private-sector Originating Initiatives

Private ICT companies around the world, including CISCO, Google, McAfee, Microsoft, Symantec, Verizon and Yahoo!, engage in hundreds of non-commercial government partnerships that offer internet safety training programs and educational literature to schools, communities and individuals. To do so, these and other companies frequently partner with organizations such as the National Cyber Security Alliance or the Family Online Safety Institute. Volunteers from the

corporations typically drive these programs and collaborate with community leaders, teachers, and the police force to deliver content.[31]

One particularly interesting private sector initiative is in combatting online child exploitation: trade in child-sex images are now annually estimated to have reached almost US$20 billion.[32] In response to pleas, Microsoft Canada developed its Child Exploitation Tracking System (CETS) software with the Royal Canadian Mounted Police (RCMP) and the Toronto Police Service following a personal email plea from Toronto Police Detective Sergeant Paul Gillespie to Microsoft Chairman and Chief Software Architect Bill Gates in January 2003.[33] CETS supports criminal investigators to efficiently organize and share media they come across during investigations, allowing units from various countries to effectively classify, track and identify links between indecent material, enabling them to identify owners and uncover international child-porn syndicates. As of March 2009, the CETS has been deployed in twelve countries and is being used by over 1200 investigators worldwide.[34] Microsoft offers the program to interested law enforcement agencies free of charge and donates all training and server software required to deploy the application at no cost.

So far, this collaborative initiative has achieved impressive results. It has been used to solve several high-profile cases and in establishing an international network of information and communications to help fight the problem. More recently, in 2008, Australian Federal Police used the CETS to smash an international pedophile internet network.[35] The investigation led to the arrest of more than twenty-two pedophiles in the United States, Canada, Australia and across Europe; the pedophiles, acting under the impression that their robust encryption codes offered sufficient protection and made them undetectable, were found out. Such collaborations help law enforcement to outsmart cybercriminals, who typically employ very sophisticated means to hide their crimes.[36]

D. Inter-governmental & International-organization Initiatives

At a macro-level, regional organizations are playing a strong role in coordinating government policy alignment and engaging corporations to address challenges. UN organizations have been particularly involved in building partnerships. For instance, UNODC has launched initiatives to engage the private sector[37] as part of its larger efforts to support UN Member States in the fight against cybercrime.[38] Similarly, ITU has launched interesting initiatives—for instance, in the Asia Pacific region, ITU helped to form the APCERT, and has partnered with national ministries of defense to create cybersecurity information sharing partnerships, such as with Japan. The ITU GCA is a five-pillared framework (legal, technical, organizational, capacity-building, cooperation) that builds on existing initiatives to improve cooperation and efficiency with and between all relevant partners.[39] Since its launch, the GCA has attracted the support and recognition of leaders and cybersecurity experts around the world.[40]

In Egypt and Turkey, where online crime is a relatively new and growing phenomenon, the CoE partners with Microsoft to conduct training with the judiciary, detailing how cybercrimes are committed and how criminals can be prosecuted, by demonstrating the most effective

methodologies for obtaining evidence. Both McAffee and Microsoft have joined forces with the CoE for a similar training in Romania. As another example, Nigeria has earned unenviable (and perhaps no longer deserved) notoriety as the hub for online scams. To break the mythology of quick financial wins through cybercrime and provide young people with a bridge to more legitimate and meaningful forms of employment, Microsoft partners with Nigerian government agencies, the European Union, UNODC and youth NGO networks to deliver online safety outreach and employability programs. The programs provide participants with broad-based ICT training, offer a recognizable certification to boost job prospects, and additional support in developing youth-driven ICT-based small business.[41]

Box 6.5: The Simda Botnet[42]

The Simda botnet, which had victims in 190 countries around the world, was successfully taken down through collaboration between INTERPOL, Trend Micro, Microsoft, Kaspersky Lab and the Cyber Defense Institute. The global dispersion of systems gathered to form the Simda botnet helped criminals commit crimes in disparate corners of the world, making it very difficult for law enforcement to combat. In a PPP with Trend Micro and Kaspersky, threat researchers working in IGCI, INTERPOL's Singapore-based center (*see* section 5 B, above), supported investigative efforts, offering expertise and access to unique threat intelligence not always available to law enforcement. With that pooled intelligence, experience and support, INTERPOL built the case for the arrest of the threat actors.

E. Initiatives in Europe

While the importance of cooperation is recognized in Europe, there is a wide diversity in national approaches and maturity levels on this issue.[43] At the European level, the CoE has engaged various corporations, including McAffee and Microsoft, to support its fight against cybercrime based on the framework of the Budapest Convention.[44] Corporate engagement is provided through training for government officials on how to effectively address threats both within national boundaries and cross-jurisdictionally.

In May 2010, the European Commission developed the Digital Agenda in May 2010.[45] The Agenda contains 101 actions grouped around seven priority areas, and operates with the dual aims of, first, improving Europe's ability to prevent, detect and, second, respond to cyberthreats, and of ensuring that digital technologies facilitate growth across the EU.[46] As a result, it is intended to strengthen the resilience of critical infrastructure, improve preparedness and promote a culture of cybersecurity through the centralization of information and the creation of PPPs.

Responding directly to recognized cyberthreats, and seeking to strengthen the EU's cybersecurity industry, the European Commission contractually established its PPP on cyberspace (cPPP) according to its Digital Single Market Strategy.[47]

The aim of the cPPP is to stimulate the European cybersecurity industry by:

1. Bringing together industrial and public resources to improve Europe's industrial policy on cybersecurity, focusing on innovation and following a jointly-agreed strategic research and innovation roadmap;
2. Helping build trust among Member States and industrial actors by fostering bottom-up cooperation on research and innovation;
3. Helping stimulate the cybersecurity industry by aligning demand and supply for cybersecurity products and services, and allowing industry to efficiently elicit future requirements from end-users;
4. Leveraging funding from Horizon2020[48] and maximizing the impact of available industry funds through better coordination and better focus on a few technical priorities; and
5. Providing visibility to European R&I excellence in cybersecurity and digital privacy.[49]

At the national level, most European nations are only at the very early stage of developing PPPs[50]; however, five countries—Austria, Germany, the Netherlands, Spain and the United Kingdom—have taken robust efforts on this front. For example, the British government has enacted the Data Protection Bill, which obliges companies to report all cyber incidents and violations, and has also launched its Cybersecurity Information Sharing Partnership (CISP), which, among other things, has led to the development of an online platform for real-time exchange of information about cyberthreats and vulnerabilities.[51] Additionally, Britain's National Crime Agency (NCA) is leading the initiative to help network administrators by developing intelligence reports for ISPs and hosting companies. The reports are based on data from Britain's national CERT (UK-CERT) and the volunteer intelligence gathering Shadowserver Foundation. The reports have identified 5,531 compromises on servers in the United Kingdom, each of which attackers can use to send spam email, launch attacks and steal information through phishing. NCA estimates organizations acting on the advice in these reports could eliminate half of phishing attacks—one of the most prevalent cyberattacks—originating from the United Kingdom. Indeed, according to one analysis, the United Kingdom ranks tenth highest for countries from which cyberattacks originate.[52] While certain elements of cybersecurity protection apply across all areas, and a wide variety of recommendations are available from national and international organizations, there is also a need for guidance that is tailored to the business needs of particular entities or provides methods to address unique risks or specific operations in certain sectors. Moreover, while there is a growing interest in establishing sector-specific responses to cybersecurity, practical implementation is still fairly limited in Member States. The same countries that are leading the way in PPPs also are the leaders in this field, often establishing sector-specific dialogues and information exchanges with the private sector. Such steps can help promote the most suitable and effective guidance throughout individual sectors.[53]

F. Initiatives in the United States of America

The US government has created many cybersecurity taskforces and interagency groups to facilitate robust information sharing not only among government agencies but also with the private sector. An example of interagency cooperation is the National Cyber Investigative Joint Task Force (NCIJTF). Led by the FBI, it is comprised of nineteen members from US intelligence and law enforcement agencies, and serves as the lead national focal point for coordinating, integrating and sharing pertinent information related to domestic cyberthreat information and national security investigations.[54]

In terms of public-private coordination, the DoD's Defense's Defense Cyber Crime Center (DC3), a military initiative, is a national center focused on addressing forensics, investigative training, research and analytics impacting those operating in the defense sector.[55] Similarly, US-CERT, housed in DHS, is the operational arm of the National Cybersecurity and Communications Integration Center (NCCIC), and plays a leading role in international information sharing.[56] DoJ's Computer Crime and Intellectual Property Section (CCIPS) works with prosecutors and agents nationally and overseas, as well as with companies and governments, to investigate and prosecute cybercrime.[57]

ISACs and the USSS's various Electronic Crimes Task Forces (ECTFs) have significantly advanced public-private information sharing.[58] For example, the ECTFs, which focus on identifying and locating international cybercriminals, have achieved significant success in detecting and apprehending numerous international cybercriminals.[59] Additionally, USSS's Cyber Intelligence Section has worked with law enforcement partners worldwide to secure the arrest of cybercriminals responsible for the thefts of hundreds of millions of credit card numbers and losses exceeding US$600 million to financial and retail institutions.[60]

Conclusion

Public-private collaboration is essential to have effective cybersecurity solutions and systems. On the one hand, the private sector brings specialized expertise and proximity to the implicated infrastructure. On the other hand, government is typically better poised to reach across borders and develop comprehensive international solutions to tracking, identifying and mitigating cyberthreats.[61]

Developing effective PPPs requires the implementation of certain fundamentals that must tie into building a strong cybersecurity framework. These range from establishing strong legal foundations and a comprehensive and regularly updated cyber security strategy, to engendering trust, working in partnership and promoting cybersecurity education. These building blocks provide valuable guidance for national governments that are ultimately responsible for implementing cybersecurity rules and policies.[62] In building systems, it is important for the private sector to be involved at the start of the process, from concept development and through implementation.

The need for PPPs in the deployment of cyber-resilience goes beyond simply partnering with the private sector. To successfully engage a widespread audience of individual consumers and small scale business operators, such partnerships need the added impetus of urgency at all levels of the critical infrastructure sphere of influence.[63] That said, partnerships should actively work to extend beyond "critical" infrastructure and actively seek to include all ICT stakeholders to create robust cyber resilience.

For PPPs to be successful, a sustained engagement and dialogue around the targeted need must be maintained. Given cultural attitudes and perspectives, the initial onus will typically be on governments, but as the incentives of government and the private sector increasingly come to align, both parties will contribute to innovative solutions. Certain tools for building partnerships—legal instruments, industry initiatives and information-sharing platforms—already exist and should be built upon. Through PPPs, existing instruments and industry standards can be used to encourage dialogue and cooperation on practical ways of dealing with cybercrime that are suitable to all. Transparency and accountability are essential elements therein.

End Notes

Referenced in: § A. The Capacity-building Challenge

1. *See* UNCTAD, *UNCTAD Information Economy Report 2015: Unlocking the Potential of E-Commerce for Developing Countries*, (New York & Geneva: UN, 2015), Ch. V, at http://unctad.org/en/PublicationsLibrary/ier2015_en.pdf
2. "Cybercrime Legislation Worldwide," UNCTAD, (2016), at http://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Cybercrime-Laws.aspx.
3. UNCTAD Global Cyberlaw Tracker, 2016.
4. *Ibid.*
5. *See* "Global Cybersecurity Index," ITU, at http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx.
6. *Ibid.*
7. For a collection of cybercrime laws, please visit the "UNODC Repository on Cyber Crime," UNODC, at https://www.unodc.org/cld/v3/cybrepo/legdb/index.html?lng=en.
8. UNODC Cybercrime Study, *supra* § 1 C, note 7.
9. "SHERLOC Portal," UNODC, at https://www.unodc.org/cld/v3/sherloc/.
10. UN Economic and Social Council, *Resolution Prevention, Protection and International Cooperation Against the Use of New Information Technologies to Abuse and/or Exploit Children*, E/RES/2011/33 (28 Jul. 2011), at http://www.un.org/en/ecosoc/docs/2011/res%202011.33.pdf.
11. Steven Malby, Tejal Jesrani, Tania Bañuelos, Anika Holterhof & Magdalena Hahn, *Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children* (Vienna: UNODC, 2011), at http://www.unodc.org/documents/organized-crime/cybercrime/Study_on_the_Effects.pdf.
12. UN Economic and Social Council, *supra* note 10.
13. "Mutual Legal Assistance Request Writer Tool," UNODC, at https://www.unodc.org/mla/introduction.html.
14. *Ibid.*
15. UNCTAD Global Cyberlaw Tracker, 2016.
16. "Summary of Adoption of E-Commerce Legislation Worldwide," UNCTAD, at unctad.org/cyberlawtracker.
17. UNODC's Global eLearning Programme has integrated the Cybercrime Repository website (http://cybrepo.unodc.org) into the cybercrime course available on the platform.
18. *See* "TrainForTrade," UNCTAD, at https://tft.unctad.org/?page_id=119.
19. UNCTAD Global Cyberlaw Tracker, *supra* note 15.
20. Uganda: National Information Technology Authority (NITA), Ministry of ICT & National Guidance, at http://www.nita.go.ug/.
21. Uganda, Ministry of ICT & National Guidance, at https://www.ict.go.ug/.
22. Uganda: Electronic Transactions Act (2011), at http://www.ulii.org/ug/legislation/act/2015/8-3; Uganda: Electronic Signatures Act (2011), at http://www.nita.go.ug/sites/default/files/Electronic-Signatures-Act.pdf.
23. NITA, "NISS Final Draft," Republic of Uganda Ministry of ICT & National Guidance, (2011), at https://www.researchictafrica.net/countries/uganda/National_Information_Security_Strategy_2011.pdf.

Referenced in: § B. Developing Capacity-building Programs

1. *See, e.g.,* UNODC, "UNODC Provided Training to South East Asian Institutions to Combat Cybercrime," (13 Oct. 2016), at https://www.unodc.org/unodc/en/frontpage/2016/October/unodc-provided-training-to-south-east-asian-institutions-to-combat-cybercrime.html; "SANS Courses," Sans, at https://uk.sans.org/courses; "Cybercrime Programme Office (C-PROC)," CoE, at http://www.coe.int/en/web/cybercrime/cybercrime-office-c-proc-.
2. David Rath, "Legislating Cybersecurity: Lawmakers Recognize Their Responsibility with Cyberthreats," Government Technology, (11 Oct. 2016), at http://www.govtech.com/security/Legislating-Cybersecurity-Lawmakers-Recognize-Their-Responsibility-with-Cyberthreats.html.
3. *See, e.g.,* Council of Europe, Law Enforcement Training Strategy, (Strasbourg: Council of Europe, 2011), at https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802f6a34; "Electronic Evidence Guide," CoE, at http://www.coe.int/en/web/octopus/home; "European Cybercrime Training and Education Group," European Cybercrime Training and Education Group (ECTEG), at http://www.ecteg.eu.
4. Joint training of prosecutors and judges may not be possible in countries where rules of ethics or statutory law prohibit as much.
5. For additional resources and examples, *see, e.g.,* "Law Enforcement – Internet Service Provider Cooperation," CoE, at http://www.coe.int/en/web/cybercrime/lea-/-isp-cooperation; CoE Project on Cybercrime and the Lisbon Network, "Cybercrime Training for Judges and Prosecutors: A Concept," (Strasbourg: CoE, 2009), at https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa3c3; CoE, Octopus Cybercrime Community, "Advanced Course for Judges and Prosecutors," at http://www.coe.int/en/web/octopus/home; Electronic Evidence Guide, *supra* note 3.
6. *See, e.g.,* "National Conference of State Legislature," National Conference of State Legislature, at http://www.ncsl.org/.
7. For additional resources and examples, *see, e.g.,* "Law Enforcement- Internet Service Provider Cooperation," CoE, at http://www.coe.int/en/web/cybercrime/lea-/-isp-cooperation; NCFTA, *supra* § 5 B, note 62.; "Financial Services-ISAC," Financial Sector Information Sharing and Analysis Center (FSIAC), at http://www.fsisac.com.
8. For additional resources and examples, *see, e.g.,* Budapest Convention, *supra* § 1 B, note 32, at Ch. 3; "24/7 Points of Contact," CoE, at http://www.coe.int/en/web/cybercrime/resources.
9. *See, e.g.,* "Action against Cybercrime," CoE, at http://www.coe.int/en/web/cybercrime.
10. *Ibid.* For an example of a quarterly update, *see* "Cybercrime at COE Update April–June 2016," CoE, at https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806931 47.
11. Convention 108, *supra* § 4 B, note 28.
12. Lanzarote Convention, *supra* § 1 C, note 7.
13. CoE, *Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism* (1 May 2008) CETS No. 198, at https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/198.
14. *See* "Cybercrime Convention Committee," CoE, at https://www.coe.int/en/web/cybercrime/tcy.
15. "Global Action on Cybercrime," CoE, at http://www.coe.int/en/web/cybercrime/glacy.
16. "Global Action on Cybercrime: From GLACY to GLACY+," CoE, at http://www.coe.int/en/web/human-rights-rule-of-law/-/global-action-on-cybercrime-from-glacy-to-glacy-.
17. "Global Project Cybercrime@Octopus," CoE, at http://www.coe.int/en/web/cybercrime/cybercrime-octopus.
18. "Regional Project Cybercrime@EaP II," CoE, at http://www.coe.int/en/web/cybercrime/cybercrime-eap-ii.
19. "Eastern Partnership, Migration and Home Affairs," European Commission, at https://ec.europa.eu/home-affairs/what-we-do/policies/international-affairs/eastern-partnership_en.
20. *Supra* note 13.
21. *See* Eastern Partnership, Migration and Home Affairs, *supra* note 14.
22. This designation is without prejudice to positions on status, and is in line with UNSC 1244 and the ICJ Opinion on the Kosovo Declaration of Independence.
23. "Cybercrime Programme Office (C-PROC)," CoE, at http://www.coe.int/en/web/cybercrime/cybercrime-office-c-proc-.
24. *See* WDR, *supra*, § 1 A, note 10.

Referenced in: § C. Private Sector Cooperation

1. US Office of Press Secretary, "Executive Order: Promoting Private Sector Cybersecurity Information Sharing," The White House of President Barack Obama, (Feb. 13, 2015) No. 13691, at https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari; Korte, *supra* § 1, note 77. In Europe, the European Commission launched a public consultation, accompanied by a policy roadmap, to seek stakeholders' views on the areas of work of a future public-private partnership, as well as on potential additional policy measures in areas such as certification, standardization, labelling that could benefit the European cybersecurity industry, *see* "Public Consultation on the Public-Private Partnership on Cybersecurity and Possible Accompanying Measures," European Commission, at https://ec.europa.eu/digital-single-market/en/news/public-consultation-public-private-partnership-cybersecurity-and-possible-accompanying-measures; European Commission, "Roadmap," Public Private Partnership on Cybersecurity, (14 Dec. 2015), http://ec.europa.eu/smart-regulation/roadmaps/docs/2015_cnect_004_cybersecurity_en.pdf. *See* Commissioner, "Digital Single Market," European Commission, http://ec.europa.eu/priorities/digital-single-market/.
2. UNODC Cybercrime Study, *supra* § 1 C, note 7, at xxv–xxvi.
3. *Ibid.*, at xxvii.
4. *See* APCERT, at https://www.apcert.org/.
5. *See* OIC-CERT, at https://www.oic-cert.org/en/.
6. *See, e.g.*, "CIRT Programme," ITU, at http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Organizational-Structures.aspx.
7. *See* "CIRT Programme," ITU, at http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Organizational-Structures.aspx.
8. Kaspersky Lab, *Kaspersky Lab Transparency Principles,* (Moscow: Kaspersky Lab., 2015), at https://cdn.press.kaspersky.com/files/2013/06/Kaspersky-Lab-Transparency-Principles_Q3_2015_final.pdf.
9. "INTERPOL Backs World Economic Forum cybercrime Project," INTERPOL, (22 Jan. 2016), ("Policing, especially in cyberspace, is no longer the exclusive preserve of law enforcement. The private sector, academia, and citizens themselves all need to be involved"), at http://www.interpol.int/News-and-media/News/2016/N2016-010.
10. *Ibid.*
11. Larry Clinton, "Cross Cutting Issue #2 How Can We Create Public Private Partnerships that Extend to Action Plans that Work?," ISA, at https://obamawhitehouse.archives.gov/files/documents/cyber/ISA%20-%20Hathaway%20public%20private%20partnerships.pdf.
12. *See* "National Cybersecurity Strategies," ITU, at http://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies.aspx.
13. *See, e.g.,* Susan W. Brenner, "Private-Public Sector Cooperation in Combating Cybercrime: in Search of a Model," Journal of International Law and Technology, Vol. 2, Issue 2, (2007), pp. 58–67, at http://www.jiclt.com/index.php/jiclt/article/view/20.
14. *See, e.g.,* Eric Luiijf, Kim Besseling & Patrick De Graaf, "Nineteen National Cyber Security Strategies," International Journal of Critical Infrastructures, Vol. 9, (2013), pp. 3–31.
15. Tarra Quismundo, "DOJ, NU Join Forces against Cybercrime," Philippine Daily Inquirer, (11 Oct. 2014), at http://technology.inquirer.net/38998/doj-nu-join-forces-against-cybercrime.
16. Jeffrey Avina, "Public-Private Partnerships in the Fight against Crime," Journal of Financial Crime, Vol. 18, Issue 3, (2011), pp. 282–29, at http://www.emeraldinsight.com/doi/pdfplus/10.1108/13590791111147505.
17. Judith H. Germano, *Cybersecurity Partnerships: A New Era of Public-Private Collaboration,* (New York: New York University School of Law, Center on Law & Security, 2014), at http://www.lawandsecurity.org/Portals/0/Documents/Cybersecurity.Partnerships.pdf. For examples of legislative efforts to promote public-private sharing of cybersecurity information in the United States, *see, e.g.,* Homeland Security Act of 2002, Pub. L. 108–275, Title II, Subtitle B, §§ 211, 116, Stat. 2135, 2150 (codified at 6 USC §§ 131–134 (2002)) (limiting the disclosure of cyberthreat information shared with the US Dept. of Homeland Security); H.R. 624, 113th Cong., at https://beta.congress.gov/bill/113th-congress/house-bill/624, (allowing for the sharing of internet traffic information between the government and technology companies); S. 2588, 113th Cong., at https://beta.congress.gov/bill/113thcongress/senate-bill/2588 (same) as cited in *ibid.*, at 16, note 1.
18. *See, e.g., United States v. Gonzalez: Indictment (charges involving cyberattacks on Heartland Payment Systems, Inc.; 7–11, Inc.; and Hannaford Brothers Co.),* (N.J.D. 2009), at http://www.wired.com/images_blogs/threatlevel/2009/08/gonzalez.pdf; *see, e.g., United States v. Gonzalez: Indictment (charges involving cyberattacks on BJ's Wholesale Club, DSW, OfficeMax, Boston Market, Barnes & Noble, Sports Authority, and several TJX companies),* (D. Mass. 2008), at http://www.securityprivacyandthelaw.com/uploads/file/2008%20Gonzalez%20Indictment.pdf; *see, e.g., United States v. Gonzalez: Superseding* (charges involving cyberattacks on Dave & Buster's, Inc.), (E.D.N.Y., 2008); *see, e.g.,* James Verini, "The Great Cyberheist," New York Times Magazine, (10 Nov. 2010), at http://www.nytimes.com/2010/11/14/magazine/14Hacker-t.html.
19. *See ibid.*
20. David Cook, "Mitigating Cyber-Threats through Public-Private Partnerships: Low Cost Governance with High Impact Returns," in *Proceedings of the 1st International Cyber Resilience Conference,* (Perth, Western Australia: Edith Cowan University, 2010), pp. 23–24, at http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1002&context=icr.
21. Some acts that might otherwise constitute cybercrime, or that with the passage of time are revealed to be acts of states against states, and that might be characterized as cyberterrorism or cyberwarfare, are beyond the scope of this Toolkit.

22. "'Security Fatigue' Can Cause Computer Users to Feel Hopeless and Act Recklessly," NIST, (4 Oct. 2016), at https://www.nist.gov/news-events/news/2016/10/security-fatigue-can-cause-computer-users-feel-hopeless-and-act-recklessly.

23. Ngair Teow-Hin, CEO of SecureAge.

24. Steven Bucci, Paul Rosenzweig & David Inserra, "A Congressional Guide: Seven Steps to US Security, Prosperity, and Freedom in Cyberspace," Heritage Foundation, at http://www.heritage.org/research/reports/2013/04/a-congressional-guide-seven-steps-to-us-security-prosperity-and-freedom-in-cyberspace.

25. *Ibid.*

26. Avina, *supra* note 16, at 288.

27. *See, e.g.,* "Microsoft Further Strengthens Security Support for Global Governments With Security Cooperation Program," Microsoft News Center, (2 Feb. 2005), at https://news.microsoft.com/2005/02/02/microsoft-further-strengthens-security-support-for-global-governments-with-security-cooperation-program/#lDhJZVyHCOTcYs68.97.

28. *See* "Microsoft Security Intelligence Report," Microsoft, Vol. 21 (14 Dec. 2016), at https://blogs.microsoft.com/microsoftsecure/2016/12/14/microsoft-security-intelligence-report-volume-21-is-now-available/.

29. "Microsoft Security Intelligence Report," Microsoft, Vol. 19, (Jan.–Jun. 2015), at http://download.microsoft.com/download/4/4/C/44CDEF0E-7924-4787-A56A-16261691ACE3/Microsoft_Security_Intelligence_Report_Volume_19_English.pdf.

30. *Ibid.*, at 6.

31. *Ibid.*

32. Internet Watch Foundation, IWF Annual Report 2008, (Cambridge: IWF, 2008), at https://www.iwf.org.uk/assets/media/IWF%20Annual%20Report%202008.pdf.

33. *See* "Microsoft Collaborates with Global Police to Develop Child Exploitation Tracking System for Law Enforcement Agencies," Microsoft New Center, (7 Apr. 2005), at https://news.microsoft.com/2005/04/07/microsoft-collaborates-with-global-police-to-develop-child-exploitation-tracking-system-for-law-enforcement-agencies/#cECWZKIO2fx3kuuZ.99.

34. Microsoft Public Sector, "Ensuring the Safety of Our Children," Microsoft, (2008), at https://www.microsoft.com/industry/publicsector/InGov/Child_Safety.aspx.

35. Frank Walker, "How Police Broke Net Pedophile Ring," Sydney Morning Herald, (23 Mar. 2008), at http://www.smh.com.au/news/national/how-police-broke-net-pedophile-ring/2008/03/22/1205602728709.html.

36. *Ibid. See also* Avina, *supra* note 16, at 289–90.

37. *See* Erwin Dotzauer, "UNODC–Comprehensive Study on Cybercrime," Cybersecurity Capacity Portal, (3 Nov. 2014), at https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/unodc-comprehensive-study-cybercrime.

38. For instance, *see* "Commission on Crime Prevention and Criminal Justice (CCPCJ)," UNODC, at http://www.unodc.org/unodc/commissions/CCPCJ/. *See also* "Crime Congress 2015: A Focus on Cybercrime," UNODC, at https://www.unodc.org/unodc/en/frontpage/2015/March/focus_its-a-crime_-cybercrime.html.

39. *See* "Global Cybersecurity Agenda (GCA)," ITU, at http://www.itu.int/en/action/cybersecurity/Pages/gca.aspx.

40. *Ibid.,* noting that H.E. Dr. Óscar Arias Sánchez, Former President of the Republic of Costa Rica and Nobel Peace Laureate & H.E. Blaise Compaoré, President of Burkina Faso, are both Patrons of the GCA.

41. Avina, *supra* note 16, at 289.

42. Jon Clay, "Operation SIMDA: The Power of Public/Private Partnerships," Trend Micro/Simply Security, (13 Apr. 2015), at http://blog.trendmicro.com/operation-simda-the-power-of-publicprivate-partnerships/.

43. "In actuality, most of the cyber security initiatives the European Commission sponsors are conducted through vessels lead by ENISA. ENISA is the European agency that has come the longest way in providing mechanisms for information sharing. By its current mandate, ENISA tackles barriers to information sharing by encouraging a homogeneous and simplified regime for 'network and information security,' '[encourage] economic growth and ensuring trust,' 'bridging the gap between technology and policy' and 'encourage and improve multi-stakeholder models which need to have a clear added value for benefiting end-users and industry,'" for details, *see* UNICRI, *Information Sharing and Public-Private Partnerships: Perspectives and Proposals,* Working Paper, (Turin: UNICRI, 2014), at http://www.unicri.it/special_topics/securing_cyberspace/current_and_past_activities/current_activities/Information_Sharing_cover_INDEXED_0611.pdf.

44. CoE, *Cybercrime: A Threat to Democracy, Human Rights and the Rule of Law,* (Strasbourg: CoE, 2009); *see also,* Budapest Convention, *supra* § 1 B, note 32.

45. "Digital Agenda for Europe," EUR-Lex, at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV:si0016.

46. *Ibid.,* at 61. For more details, *see* "DG Connect," European Commision, at https://ec.europa.eu/digital-single-market/dg-connect.

47. *See* "Digital Single Market," *supra* note 1.

48. *See* "Horizon 2020," European Commission, at https://ec.europa.eu/programmes/horizon2020/

49. *See* "Digital Single Market: Bringing Down Barriers to Unlock Online Opportunities," European Commission, at http://ec.europa.eu/priorities/digital-single-market/.

50. BSA (Business Software Alliance), *EU Cybersecurity Dashboard: A Path to a Secure European Cyberspace,* (Washington DC, 2015), http://www.bsa.org/~/media/Files/Policy/Security/EU/study_eucybersecurity_en.pdf; Warwick Ashford, "Co-Operation Driving Progress in Fighting Cyber Crime, Say Law Enforcers," Computer Weekly, (5 Jun. 2015), at http://www.computerweekly.com/news/4500247603/Co-operation-driving-progress-in-fighting-cyber-crime-say-law-enforcers.

51. "Government Launches Information Sharing Partnership on Cyber Security," Government of the United Kingdom, Press Release, (23 Mar. 2013), at https://www.gov.uk/government/news/government-launches-information-sharing-partnership-on-cyber-security.

52. *See* "Live Cyber Attack Threat Map," Threatcloud, at https://threatmap.checkpoint.com/ThreatPortal/livemap.html.

53. Clay, *supra* note 42, at 61.

54. "National Cyber Investigative Joint Task Force," FBI, at https://www.fbi.gov/about-us/investigate/cyber/ncijtf.

55. "DoD Cyber Crime Center (DC3)," US Dept. of Defense, at http://www.dc3.mil/.

56. "US-CERT: About Us," US CERT (Computer Emergency Readiness Team), at https://www.us-cert.gov/about-us.

57. "Computer Crime & Intellectual Property Section (CCIPS): About the Computer Crime & Intellectual Property Section," US Dept. of Justice, at https://www.justice.gov/criminal-ccips.

58. *See, e.g.*, Mary Kathleen Flynn, "ISACs, Infragard, and ECTF: Safety in Numbers," CSO, (8 Nov. 2002), at http://www.csoonline.com/article/2113264/security-leadership/isacs--infragard--and-ectf--safety-in-numbers.html.

59. Germano, *supra* note 17 at p. 13.

60. *Ibid.*, at 18, note 55.

61. *Ibid.*, at 2.

62. Thomas Boué, "Closing the Gaps in EU Cyber Security," Computer Weekly, (Jun. 2015), at http://www.computerweekly.com/opinion/Closing-the-gaps-in-EU-cyber-security.

63. Avina, *supra* note 16.

CHAPTER 7

In-country Assessment Tool

This chapter provides an overview of various existing tools to use in conducting assessments of cybercrime preparedness (mainly those of the participating organizations) and introduces the Assessment Tool developed as a part of the Toolkit. As explained in further detail in the chapter, the Assessment Tool synthesizes various aspects of other existing instruments to enable users to determine gaps in capacity and highlight priority areas to direct capacity-building resources.

In this Chapter

A. Assessment Tool—Overview

Table of Contents

Introduction

The first part of the Toolkit (chapters 1 to 6) provides resources and context for building-capacity to combat cybercrime, presenting the various issues related to cybercrime. This second part of this Toolkit is more interactive, providing an overview of existing tools used to make cybercrime preparedness assessments and introducing the synthetic Assessment Tool that has been developed under this Project. It begins with **(I)** an overview of the Toolkit's assessment tool (Assessment Tool), and concludes with **(II)** a summary of the Assessment Tool.

I. Overview of the Toolkit's Assessment Tool

The focus of the Toolkit is developing country capacity to combat cybercrime. Although perhaps axiomatic, capacity needs to be assessed before capacity-building priorities can be identified or resources can be allocated. Accordingly, this section **(A)** reviews some of the existing assessment tools—notably those used by organizations participating in this Project (AIDP, CoE, ITU, KSPO, Oxford, UNICRI and UNODC), but also those of others (notably INTERPOL and OAS)—, and then **(B)** describes the purpose, structure and methodology proposed by the Assessment Tool.

A. Existing Assessment Tools

A number of the Toolkit's participating organizations have their own cybercrime assessment tools.[1] While there is some overlap of issues addressed by each of them, each organization's assessment was designed for a specific purpose and assesses cybercrime from different aspects. The tables provided in appendix 9 D identify each topic or issue being assessed by each assessment and also shows whether that topic or issue is addressed by one or multiple assessment tools. As can be seen from reviewing appendix 9 D, there is considerable common ground covered by each of the different assessment tools—for example in the areas of enactment of laws, definitions of cybercrime and certain procedural issues, to name a few. Conversely, the tables of the appendix also show that not all assessments cover all subjects.

In light of various means of assessing cybercrime, and of its diverse impacts,[2] it is worth presenting a brief synopsis, in chronological order, highlighting the different areas of the focus and orientation of each of the participating organizations' assessment tools:

- **AIDP:** AIDP's assessment tool is in the form of "questionnaire", and was developed in 2012 to 2013 following sections I to IV of AIDP's Preparatory Colloquia for the Nineteenth International Congress of Penal Law on "Information Society and Penal Law".[3] These questionnaires are designed to elicit a narrative response to each question.

- **CoE:** The CoE assessment tool, also in the form of a "questionnaire" or country profile, was prepared in 2007 in connection with CoE's Octopus Conference on "Cooperation against Cybercrime" (*see* section 6 B, above).[4] This tool aims to assess domestic laws' compliance with provisions of the Budapest Convention.[5]

- **ITU:** The ITU assessment tool, presented in the form of a "country work sheet", was developed in 2010.[6] Its aim is to enable provisions of domestic laws consistent with those of sample legislative language in the ITU Toolkit for Cybercrime Legislation.[7] Neither the CoE nor the ITU assessment tools contain questions regarding to either rules on e-evidence, or to cybercrime issues arising outside of legal frameworks.

- **UNODC:** The UNODC assessment tool, prepared also in the form of a "questionnaire", was developed in 2012 in preparation for its Comprehensive Study on Cybercrime.[8] The UNODC assessment tool is designed to holistically assess both legal and non-legal frameworks for addressing cybercrime issues, along with a country's capacity to investigate, to prosecute and to try cybercrime cases.

- **Oxford's GCSCC:** The Global Cyber Security Capacity Centre (GCSCC) of Oxford University's Martin School has developed a comprehensive "maturity model" assessment tool that was launched in 2014.[9] The purpose of the maturity model is aimed at making it possible for countries to evaluate their level of preparedness with respect to a variety of dimensions of cybersecurity by allowing them to self-assess their current cybersecurity capacity. The maturity model assesses cybercrime as part of a broader assessment of a country's cybersecurity preparedness.

In addition, the Project evaluated the assessment methodologies of INTERPOL and the OAS. A brief synopsis of the salient features of these follows:

- **INTERPOL:** INTERPOL conducts two types of assessments for its members: first, an on-request "National Cyber Review" that assesses different aspects of a country's ability and institutional and human-capacity to investigate and prosecute cybercrimes and an assessment of threat levels; second, "Rapid Cyber Assessments" that focus on a country's operational readiness to combat cybercrime.
- **OAS:** The OAS Cybercrime Questionnaire[10] assesses whether OAS Member States have substantive and procedural cybercrime legislation, as well as some institutional attributes. Relatedly, OAS, together with the Inter-American Development Bank (IADB), publishes a country-by-country reviews of OAS Member State cybersecurity readiness utilizing the Oxford methodology in its 2016 Cybersecurity Report *Cybersecurity: Are we ready in Latin America and the Caribbean?*[11] This is a broader cyber-security review, and not a cybercrime specific review.

B. Developing a Synthetic Assessment Tool

The overall purpose of the Toolkit is to identify and examine international good practices and to bring together, perhaps in ways that they have not been so in the past, different aspects of providing assistance to developing countries in the fight against cybercrime. In so doing, the Toolkit incorporates information and experience from cases and looks at not only new and evolving means of committing cybercrimes (*e.g.,* financial crimes and child pornography), but also at new, evolving and perhaps even non-traditional ways of combatting cybercrime (*e.g.,* reliance on data provided by the private sector and novel formal and informal means of cooperation with the private sector). Further, the Toolkit is not aimed at duplicating existing efforts but at providing *nexi* for synergizing various existing approaches, taking the best from various sources and combining them in a way that perhaps has not been done before. This approach and ethos also underlays the synthetic Assessment Tool developed by the Project that can be found in appendix 9 E.

The Assessment Tool is topically organized according to the general structure that can be found in the table of contents of the Toolkit. Using this thematic structure, the Project examined the existing assessment tools mentioned above, identifying both common ground and certain gaps. The Assessment Tool attempts to address capacity building to combat cybercrime in a holistic fashion. Furthermore, while the focus of the Toolkit is on policy, legal and law-enforcement issues, it was recognized that, in order to be as useful as possible, a more comprehensive tool going beyond assessing merely "legal" issues would be needed.

At that same time, methodologically, the Assessment Tool attempts to bring in good practices from a number of sources, in particular Oxford's aforementioned maturity-model approach to cybersecurity capacity-building assessment,[12] but focusing on "objective" rather than subjective analyses. One limitation of many of the assessments reviewed (including the Assessment Tool), is

that it does take a certain amount of assumed knowledge of the subject matter in order to be able to actually assess a response to the various criteria—a need which the Project aims to fill through the text and discussion found in the first part of the Toolkit. Furthermore, many of the criteria assessed in the existing assessments reviewed require subjective judgements.

Accordingly, the challenge of developing the Assessment Tool was to retain the richness of the maturity-model approach but to limit the subjectively-based criteria and responses of some of the existing assessments.

Objectivity, richness and accessibility are all needed to make an assessment tool effective and universally-applicable, all of which are key considerations of the Assessment Tool:

- **Objectivity** is achieved by making the response to each question in the Assessment Tool a binary, "yes/no" response to the greatest extent possible, or to create a clear choice along a small-scale of options.
- **Richness** is achieved by "weighting" each criterion. The Assessment Tool uses approximately 115 indicators grouped into nine themes (or dimensions).
- **Ease-of-comprehension** is achieved through graphic representations of In order to graphically show where a country's capacity-building resources, showing—in one picture—all of the thematic areas in a single "spider" chart. That chart shows, relative to the other thematic areas, how a country fares with respect to each criterion or dimension. Each theme on the general spider chart can also be drilled -down to a more granular level showing performance on each of the different sub-criteria.

The combination of these three elements facilitates policy, law and decision makers to best decide how resources should be allocated, while first-time users of the Assessment Tool may require some guidance, it is anticipated that the Assessment Tool is relateively straightforward and that it could be used in subsequent years to periodically measure progress.

II. Summary of the Assessment Tool

A. What Is Covered & How It Works

The Assessment Tool is organized along the following lines. First, basic structure begins with policy assessment, before moving on to consider legislation (both substantive and procedural law), then going on to safeguards, MLA and, finally, institutional matters.

As possibly evident, the Tool takes inspiration for its architecture from the topics that are covered in the Toolkit, in some form or another, as well as from the other assessments mentioned above.

Conceptually, the Assessment Tool's 115 indicators are organized around the following nine dimensions:

- **Non-Legal Framework,** covering national strategies and policies and other matters of a non-legal nature such as cooperation with the private sector;
- **Legal Framework,** covering national law and whether a country has joined a treaty;
- **Substantive Law,** addressing activities that have been criminalized;
- **Procedural Law,** mainly addressing investigatory matters;
- **e-Evidence,** focusing on admissibility and treatment of digital evidence in the cybercrime context;
- **Jurisdiction,** focusing at how the jurisdiction of the crime is determined;
- **Safeguards,** focusing on three elements—"due process", data protection and freedom of expression[13];
- **International Cooperation,** focusing on, first extradition, and, second, on both formal and informal levels of MLA; and
- **Capacity-building,** looking at both institutional (*e.g.,* law enforcement training academies) and human capacity-building focusing on training needs for law enforcement, prosecution and the judiciary.

It bears noting that in three dimensions—Legal Framework, Substantive Law and Procedural law—no distinction is made between whether there is a bespoke cybercrime law or whether provisions regarding cybercrimes are found in a general criminal law.

B. Other Features of the Assessment Tool

Importantly, the Assessment Tool is not expected to be or result in a ranking of countries. While the Assessment is available as part of the Toolkit, is available as a stand-alone instrument freely available on the internet (www.combattingcybercrime.org) for anyone to use.

The results of the Assessment Tool will also be confidential to those choosing to use it (*i.e.,* if a country does an assessment of its capacity to combat cybercrime, those results will be only available to the person or entity making the assessment). A country can choose to release the results of the assessment if it chooses. However, as the Assessment Tool is publicly and freely available, it will be an instrument of transparency and contestability.

Moreover, to ensure accountability, anyone can download the Assessment Tool and do an assessment of a country's preparedness to combat cybercrime. The Assessment Tool also acts as a kind of "due diligence" checklist for countries contemplating elaborating policies and legislation to combat cybercrime.

Conclusion

The Project's Assessment Tool is a synthesis of the various assessment tools used by a number of institutions, many of whom have contributed to, and partnered in, its development. The Tool is not intended to duplicate efforts but to provide *nexi* for synergizing various existing approaches.

The Tools seeks to present an assessment that is objective (through clear-choice answers), information-rich (through weighted criteria) and easy to comprehend (through graphic representations). It considers policy and legislation, takes account of actual cases and brings together international good practices. The aim is to give countries the means for holistically building their capacity to fight cybercrime. The Tool's structure parallels that of the chapters of the Toolkit, to which reference should be made for further elucidation and understanding of the aspects that are being assessed.

End Notes

Referenced in: § A. Assessment Tool—Overview

1. A full list of the existing tools of participating organizations can be found in appendix 9 D.
2. *See, e.g.,* WDR, *supra* § 1 A, note 10, at 222 et seq.
3. *See, e.g.,* endnote "i" in appendix 9 D.
4. *See, e.g.,* endnote "ii" in appendix 9 D.
5. *See* Budapest Convention, *supra* § 1 B, note 32.
6. *See, e.g.,* endnote "iii" in appendix 9 D.
7. ITU, *Toolkit for Cybercrime Legislation* (Feb. 2010), at http://www.cyberdialogue.ca/wp-content/uploads/2011/03/ITU-Toolkit-for-Cybercrime-Legislation.pdf; *see also* ITU, Global Cybersecurity Index (GCI), (2014), at https://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI-2014.aspx. The 2016 GCI, though focusing more broadly on issues of cybersecurity, also presents issues related to cybercrime preparedness. *See* ITU, Global Cybersecurity Index (GCI) 2015/16 Questionnaire Guide," at https://www.itu.int/en/ITU-D/Cybersecurity/Documents/QuestionnaireGuide-E.pdf.
8. *See, e.g.,* endnote "v" in appendix 9 D. *See* also Comprehensive Study on Cybercrime, *supra* § 1 C, note 7.
9. GCSCC Maturity Model [hereafter, "Oxford"], at https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM%20Version%201_2_0.pdf.
10. *See, e.g.,* "Questionnaire Related to the Recommendations from the Fourth Meeting of Governmental Experts on Cyber-Crime," OAS, (2006), at http://www.oas.org/juridico/english/cybGE_IVquest.doc.
11. OAS & IADB, 2016 Cybersecurity Report, *Cybersecurity: Are We Ready in Latin America and the Caribbean?,* at https://goo.gl/4UUfwQ.
12. *See,* Oxford, *supra* note 9.
13. Indeed, there may be other basic due process issues to be addressed as well. These are included in the "Procedural" section of the Assessment Tool. As structured, the Assessment Tool breaks out under "safeguards" the two issues—data protection (privacy) and freedom of expression.

CHAPTER 8

Analysis & Conclusion

This final chapter offers some concluding thoughts on evolving good practices in combatting cybercrime.

In this Chapter

A. Analysis & Conclusion

Table of Contents

Introduction

The Toolkit, as well as its accompanying Assessment Tool and virtual library,[1] are aimed at addressing the capacity-building needs of countries with developing economies in the legal aspects of the global fight against cybercrime. It recognizes that a variety of stakeholders—both public and private—are involved in different aspects of this struggle. As the recent WannaCry[2] and Petya[3] ransomware attacks underscore, cybercrime is a global and pervasive threat, intimately intertwined with virtually every sector, from finance to health to ICT. The needs and challenges in the investigation and prosecution of cybercrime apply *modus modendi* to any type of crime involving electronic evidence.

Cybercrime is no longer an isolated concern, and combatting it is no longer realistic without a comprehensive, collaborative, global approach. Indeed, global-cybersecurity awareness, training and capacity-building are critical in this interconnected world.

In attempting to bolster capacity in the struggle against global cybercrime, the Toolkit attempts to provide insight into a range of questions:

- What is cybercrime?
- How is cybercrime addressed in national policy and legislation?
- What, given cybercrime's global nature, are good practices for formal international cooperation?
- What informal cross-border cooperative methods can be encouraged?
- What are some of the safeguards in place that balance security with due process and rule of law?
- What are some of the challenges facing capacity-building initiatives, and what efforts are being made to address those challenges?
- What tools are there for countries to assess their capacity-building priorities?

In addressing some of these foundational questions, the appendices to the Toolkit also provide reference materials regarding selected recent cases that interpret national cybercrime laws, a compilation of nations' laws on cybercrime, international instruments addressing cybercrime and other existing assessment tools.

In building capacity to combat cybercrime, both international and domestic law issues must be taken into account. Additionally, there is a complementarity to be maintained between the security that comes from effective prosecution of cybercrimes, on the one hand, and the interests of due process, data protection and access to information, on the other.

I. Challenges—Known, New & Evolving

Throughout, the Toolkit explores the myriad challenges of developing building-capacity to combat cybercrime, and does so from multiple perspectives. On the legal front, combatting cybercrime involves a mixture of both domestic and international law and policy: However, that mixture is a complex one. Moreover, despite the fact that many countries have cybercrime laws, a host of other complicating factors, such as the lack of a common treatment of what is criminalized, leads to problems of interoperability, and therefore to complications in cross-border cooperation. Furthermore, technological advances continue to complicate matters.

"New" technologies and approaches, such as cloud services and distributed or shared-ledger technology (such as blockchain), may offer users and industry important boons; at the same time, however, those very same technologies may be exploited by criminals, thus posing new and additional capacity-building challenges.

- **Cloud services:** Centralized data storage and processing pose challenges on a variety of fronts. Jurisdictionally, because, first, the physical site of the cloud facility's servers may not be in the same jurisdiction as either the crime or the victim, and, second, the state in which the cloud facility's servers are geographically located may not similarly criminalize the activity as the jurisdiction of either the crime or its victim—that is, the essential requirement of "dual criminality", upon which cross-border cooperation is typically premised, may not be in place (*see* section 2 A, above), thereby hindering interoperability from the start (*see* section 2 E, box 2.6). Furthermore, for a host of reasons, the distributed technology of shared ledgers may also make investigations more difficult. Both centralized and distributed technologies make the process of "attribution" of criminal actions more challenging.
- **"Policing":** Making cybercrime more expensive for cybercriminals is increasingly evolving from efforts focused on "prosecution" to "prevention". Efforts that include policing of activities by third-party, private-sector and service providers are also considered under this category.[4] Similarly, in terms of managing liability to cover the costs of cybercrime, it is possible to conceive of "privatizing" the costs of combatting cybercrime by imposing liability on manufacturers of "insecure" devices.[5]

- **State-actor cyber-interventions:** Finally, and although beyond the scope of the Toolkit, it bears noting that the rise of state-actors in cyber activities that, in a non-military context would be considered cybercrime, has resulted in an increased blurring of the lines between cybercrime and cyberwarfare.[6]

II. Collaboration & Coordination

Much of the Toolkit's focus has been on the importance of collaboration and coordination among actors in combatting cybercrime. International organizations, some of whom have participated in the elaboration of this Toolkit and the Assessment Tool, such as CoE, ITU, UNCTAD and UNODC, are working towards providing and sharing open tools and other resources with governments and other stakeholders, sometimes through including the resources of other organizations in addition to their own. Still other international organizations, such as the Commonwealth, are supporting and facilitating communication between their Member States. An ever-increasing number of tools are being made available–for example, by the OAS–for governments, therein enabling them, first, to identify their needs and, second, to develop their own counter-cybercrime strategies, complete with means for establishing baselines to measure their progress. And new partnership initiatives between civil society, the private sector and international or regional organizations, such as INTERPOL, are resulting in the forging of joint -ction plans. At the CoE, the State Parties to the Budapest Convention meet twice per yearly to review the implementation of the Budapest Convention and to negotiate solutions to address emerging challenges. More in-depth studies, such as those done through Chatham House, are being developed, having the aim of bridging gaps between policy and technology experts and of keeping stakeholders abreast of how cybercrime develops. Inexpensive online tools for capacity-building are being made available for law enforcement agencies, prosecutors and lawyers, guaranteeing sustainability and a wider reach. Efforts at harmonizing and creating common approaches to cybercrime issues, such as evidence, are facilitating criminal investigations. All of these effprts are essential to combatting cybercrime.

Conclusion: The Way Forward

Cybercrime not being an isolated concern, it can only be combatted through a comprehensive, collaborative, global approach, which necessities global cybersecurity awareness and global capacity-building. Such a vision is increasingly emerging and, in these times of progressive partnerships and rapid technological development, so, too, is international interoperability increasingly emerging. Additionally, just as technological developments increasingly make interconnected-efforts and shared operations possible, so, too, do they present increased potential for cybercriminals, thus requiring greater legal malleability, a further factor that must be included in advancing developing that global cybersecurity effort.

Even as these collaborative and cooperative initiatives are being undertaken, it bears emphasizing that it is increasingly being recognized that combatting cybercrime is not a one-size-fits-all proposition. A tailored, setting-sensitive approach must be taken.

Moreover, there is also recognition of the need to avoid duplicating existing efforts. One challenge, of course, is that, as organizations pursue their respective mandates, they also attempt to synthesize and to build upon existing work within the scope of their mandate.[7] Coordination between actors is an ongoing and continuing effort. As such, awareness-raising, information-exchange and capacity-building continue to be main priorities around which organizations are partnering.

Lastly, such collaboration and cooperation must not only account for the various strengths of each organization offering support, but must also account for, and be sensitive to, client needs. Such sensitivity can best be inculcated through client ownership.[8] As those two parts of the puzzle are increasingly put in place, international interoperability and a shared effort to combat cybercrime is increasingly emergent.

End Notes

Referenced in: § A. Analysis & Conclusion

1. The Assessment Tool is described in detail in section 7. The Toolkit, Assessment Tool and virtual library are all available at www.combattingcybercrime.org.
2. *See supra* § 1 C, box 1.2.
3. *See, e.g.,* Kevin Conklin, "The Petya Virus—Return of the Ransomware Attacks," Information Management, (Jun. 2017), at https://www.information-management.com/opinion/the-petra-virus-return-of-the-ransomware-attacks.
4. Remarks delivered by Ian Walden at "Cybersecurity and Cybercrime: New Tools for Better Cyber Protection," UNTAD e-Commerce Week (Geneva: UNCTAD, 24–28 Apr. 2017), at http://unctad.org/meetings/en/Presentation/dtl_eWeek2017p07_IanWalden_en.pdf.
5. *Ibid.*
6. WDR, *supra* § 1 A, note 10, at 222. While such actions "blur[ ] the lines between acts of cybercrime and cyberwar or cyberterrorism," it is nonetheless the responsibility of the government to assure public safety and security in cyberspace. *Ibid.* at 223. *See also supra* § 2 F. The spectrum of such activities ranges vastly, from actions affecting private entities and individuals that might more strictly and more straightforwardly be understood as cybercrime if a state-actor were not involved (*e.g.,* hacking, data theft), to more aggressive activities that might better be understood as cyberwarfare (*e.g.,* targeting nuclear facilities). In certain instances, states are taking to airing grievances openly, and even taking legal action to combat against such activities: for instance, in the United States, a grand jury recently indicted four defendants, including two Russian Federal Security Service (FSB) agents, for "computer hacking, economic espionage and other criminal offenses in connection with a conspiracy, beginning in January 2014, to access Yahoo's network and the contents of webmail accounts." US Dept. of Justice, Office of Public Affairs, "U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts," (15 Mar. 2017), at https://www.justice.gov/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions. *See also United States v. Dmitry Dokuchaev, et al.,* CR17-103 (N.D. Cal. 2017), at https://www.justice.gov/opa/press-release/file/948201/download. For a discussion of the larger implications of instances tending towards what might be construed as cyberwarfare and government responsibility for accounting for such matters, *see, e.g., supra* § 2 F; *see also,* Nicole Perlroth, "Hackers Are Targeting Nuclear Facilities, Homeland Security Dept. and F.B.I. Say," New York Times, (6 Jul. 2017), at https://www.nytimes.com/2017/07/06/technology/nuclear-plant-hack-report.html?mcubz=0.
7. As Sir Isaac Newton said, "If I have seen further it is by standing upon ye shoulders of Giants." Letter to Robert Hooke (15 Feb. 1676).
8. *See supra* § 6 B.

Appendices

The following appendices provide additional detailed "meta" information discussed in the preceding chapters of the Toolkit.

In this Chapter

A
APPENDIX
TABLE A

Cybercrime Related to Financial Institutions with Direct Costs

Explanatory Note: This Appendix lists cases intended to capture the issues addressed in this Toolkit, including both the challenges and complexities of addressing cybercrime, as well as successes that can be achieved through multi-jurisdictional and private sector cooperation. The cases are illustrative (and by no means exhaustive) and were gathered from credible public and private sector open sources. The cases reviewed are primarily from the following jurisdictions: Australia, Canada, Germany, Japan, Korea, Russia, Switzerland, Ukraine, United Kingdom and the United States. The Appendix analyzes the cases looking at the characteristics of the attackers; the origin and target jurisdiction; the targets of the attack; the amount involved or stolen; the mode/methodology of attack; whether they were any indictments on the alleged attackers; the legal basis for any indictments; and the sources for the case information. A number of the cases shown in this Appendix correspondents to the references used in the text of the Toolkit. Cases appearing in the Toolkit highlight five critical issues: 1) the direct and indirect monetary implications of the attacks on financial and non-financial institutions; 2) the different approaches on the legal basis for charging alleged criminals (some cases use specific anti-cybercrime legislation, others use anti-money laundering law, and still others use violation of some underlying statute using a computer network); 3) some cases illustrate the cross-border nature of cybercrime (inevitably requiring that in order to conduct successful investigations, countries will have to cooperate); 4) space/forum has to be created that brings together the public and private sectors to collaborate in investigating cybercrime threats; and 5) the means used to carry out the cyberattacks, include malware, phishing schemes and social engineering, hacking, botnet, distributed denial of service and many other methods.

Cybercrime Related to Financial Institutions with Direct Cost							
Cyber Crime Case	**Affected Jurisdictions**	**Target(s) of attack**	**Damages Incurred**	**Responding Entity**	**Indictment(s)**	**Case information** (legal provision that case was charged under)	**Resources**
Carbanak (Anunak is the name of the malware author that is often mentioned **alongside** this case) (Jan. 2013-present)	**Origin:** Unclear **Target:** Banks in Russia, Japan, the Netherlands, Switzerland, the U.S. and others.	Banks (100 banks and other financial institutions in 30 nations)	$300 million - $1 billion	Kaspersky Lab, INTERPOL, Europol, and authorities from various nations.	N/A	N/A	http://www.securityweek.com/hackers-hit-100-banks-unprecedented-1-billion-cyber-attack-kaspersky-lab http://25zbkz3k00wn2tp5092n6di7b5k.wpengine.netdna-cdn.com/files/2015/02/Carbanak_APT_eng.pdf http://www.nytimes.com/2015/02/15/world/bank-hackers-steal-millions-via-malware.html http://www.nytimes.com/2015/02/15/world/bank-hackers-steal-millions-via-malware.html?partner=socialflow&smid=tw-nytimes&_r=2

A
APPENDIX
TABLE A

Cybercrime Related to Financial Institutions with Direct Costs

Continued from last page

Cybercrime Related to Financial Institutions with Direct Cost							
Cyber Crime Case	**Affected Jurisdictions**	**Target(s) of attack**	**Damages Incurred**	**Responding Entity**	**Indictment(s)**	**Case information** (legal provision that case was charged under)	**Resources**
Bangladesh Central Bank Reserve Hack (Feb 2016)	**Origin:** Unclear but stolen funds were transferred to accounts in the Phillipines. **Target:** U.S.	Federal Reserve Bank of New York	$100 Million	Bangladesh government reported the missing funds to the U.S. Federal Reserve.	N/A	N/A	http://www.bbc.com/news/business-35809798 https://www.bloomberg.com/news/articles/2016-03-08/u-s-fed-responsible-for-missing-100-million-bangladesh-says
Carberp Trojan (2009-2013)	**Origin:** Ukraine (Kiev, Zaporzhe, Lyov, Odessa and Kherson) **Target:** Ukrainian and Russian	Ukrainian and Russian Banks	$250 million	Joint operations by the Security Service of Ukraine and the Russian Federal Security Service	N/A	N/A	http://www.securityweek.com/source-code-carberp-trojan-sale-cybercrime-underground http://www.securityweek.com/russian-authorities-claim-capture-mastermind-behind-carberp-banking-trojan http://translate.google.com/translate?sl=ru&tl=en&js=n&prev=_t&hl=en&ie=UTF-8&eotf=1&u=http%3A%2F%2Fwww.kommersant.ua%2Fdoc%2F2160535

A
APPENDIX
TABLE A

Cybercrime Related to Financial Institutions with Direct Costs

Continued from last page

Cybercrime Related to Financial Institutions with Direct Cost							
Cyber Crime Case	**Affected Jurisdictions**	**Target(s) of attack**	**Damages Incurred**	**Responding Entity**	**Indictment(s)**	**Case information** (legal provision that case was charged under)	**Resources**
Gameover Zeus (2012)	**Origin:** Russia, Ukraine and U.K. **Target:** U.S.	individual computers, information therein and financial institutions.	$100 million	FBI, law enforcement from the Australian Federal Police; the National Police of the Netherlands National High Tech Crime Unit; European Cybercrime Centre (EC3); Germany's Bundeskriminalamt; France's Police Judiciare; Italy's Polizia Postale e delle Comunicazioni; Japan's National Police Agency; Luxembourg's Police Grand Ducale; New Zealand Police; the Royal Canadian Mounted Police; Ukraine's Ministry of Internal Affairs – Division for Combating Cyber Crime; and the United Kingdom's National Crime Agency participated in the operation. The Defense Criminal Investigative Service of the U.S. Department of Defense also participated in the investigation.	The indictment for the creator of the malware: http://www.justice.gov/sites/default/files/opa/legacy/2014/06/02/pittsburgh-indictment.pdf http://www.justice.gov/opa/documents-and-resources-june-2-2014-announcement	GameOver Zeus is an extremely sophisticated type of malware used to steal banking and other credentials from the computers it infects. Infected computers, unbeknownst to the owners, become part of a botnet that uses the stolen credentials to initiate wire transfers to the accounts overseas owned by criminals. Evgeniy Bogachev, the creator of the malware, received one 1 count conspiracy, 1 count of wire fraud, 1 count of computer fraud, 9 counts of bank fraud, and 2 count of money laundering.	https://www.fbi.gov/news/stories/malware-targets-bank-accounts https://www.fbi.gov/file-repository/gameoverzeus_v13_fullgraphic_web_opt2.pdf
Operation High Roller (January 2012 to April 2012)	**Origin:** Hosting locations and command and control servers mainly located in Russia, with some in the U.S., Germany, Italy, Ukraine and China. **Target:** Mainly U.S., Europe, Columbia	Boutique Financial Institutions, credit unions, large global banks and regional banks.	Estimated $78 million stolen with potenitally 2 billion euros in attempted fraud.	Identified by McAfee and Guardian Analytics. Subsequently pursued by relevant authorities.	N/A	N/A	http://www.scmagazine.com/racket-drains-high-roller-bank-accounts-in-automated-style/article/247542/ http://www.reuters.com/article/2012/06/26/us-online-bankfraud-idUSBRE85P04620120626 http://blogs.wsj.com/cio/2012/06/26/operation-high-roller-targets-corporate-bank-accounts/ https://www.finextra.com/finextra-downloads/newsdocs/high-roller.pdf

A
APPENDIX
TABLE A

Cybercrime Related to Financial Institutions with Direct Costs

Continued from last page

Cybercrime Related to Financial Institutions with Direct Cost							
Cyber Crime Case	**Affected Jurisdictions**	**Target(s) of attack**	**Damages Incurred**	**Responding Entity**	**Indictment(s)**	**Case information** (legal provision that case was charged under)	**Resources**
SpyEye 2009-2011. (potentiallty still active: 10,000 bank accounts had been compromised by it in 2013)	**Origin:** Atlanta, Georgia. U.S. **Target:** Multinational	Victims' bank accounts.	Panin was on Interpol redlist for banking scams stealing more than $5 million. The malware was mainly sold and used by others. 'soldier' stole more than $3.2 million during a 6 month period in 2011.	Investigated by the FBI. Assisted by the United Kingdom's National Crime Agency, the Royal Thai Police-Immigration Bureau, the National Police of the Netherlands-National High Tech Crime Unit (NHTCU), Dominican Republic's Departamento Nacional de Investigaciones (DNI), the Cybercrime Department at the State Agency for National Security-Bulgaria, and the Australian Federal Police (AFP). Private sector: Trend Micro's Forward-looking Threat Research (FTR) Team, Microsoft's Digital Crimes Unit, Mandiant, Dell SecureWorks, Trusteer, and the Norwegian Security Research Team known as Underworld.no.	http://krebsonsecurity.com/wp-content/uploads/2014/01/Panin-Indictment.pdf	11 counts of Computer Fraud and Abuse, 1 count of Copmputer Fraud and Abuse conspiracy, 10 counts of wire fraud, 1 count of wire and bank fraud conspiracy.	http://www.bbc.com/news/technology-25946255 http://www.wired.com/2014/01/spy-eye-author-guilty-plea/

A
APPENDIX
TABLE A

Cybercrime Related to Financial Institutions with Direct Costs

Continued from last page

Cybercrime Related to Financial Institutions with Direct Cost							
Cyber Crime Case	**Affected Jurisdictions**	**Target(s) of attack**	**Damages Incurred**	**Responding Entity**	**Indictment(s)**	**Case information** (legal provision that case was charged under)	**Resources**
Jabber Zeus Crew (Fall 2010)	**Origin:** Ukraine, Russian and the U.K. **Target:** U.S.	Bank accounts of medium sized businesses, towns and churches.	$70 million stolen ($220 million attempted)	Colloaborative law enforecment effort which partnered U.S. governmental entities with their counterparts in the United Kingdom, Ukraine, and Netherlands.	http://www.justice.gov/iso/opa/resources/5922014411104621620917.pdf	For malicious activities dating as far back as 2009, all the individuals are charged with conspiracy to participate in racketeering activity, conspiracy to commit computer fraud and identity theft, aggravated identity theft, and multiple counts of bank fraud	http://www.scmagazine.com/indictment-charges-jabber-zeus-crew-with-using-malware-to-steal-millions/article/342375/ http://www.fbi.gov/news/stories/2010/october/cyber-banking-fraud http://www.securityweek.com/zeus-source-code-leaked-really-game-changer
Coreflood (2009-2011)	**Origin: Search warrants were issued for control and command servers in Arizona, Georgia, Texas, Ohio, and California.** **Target:** U.S.	Company information (Michigan, South Carolina, North Carolina, Connecticut, Tenessee)	$600,000 (1.5 million attempted)	DOJ was able sieze domain names and to later decomission the botnet through the use of the NPO Internet Systems Consortium (ISC). FBI's New Haven Division led the investigation, in coordination with the U.S. Marshals Service. Microsoft, the Internet Systems Consortium, and other private industry partners also contributed. The case is being prosecuted by the U.S. Attorney's Office for the District of Connecticut, and attorneys from the Computer Crime and Intellectual Property Section in the Justice Department's Criminal Division	https://www.fbi.gov/newhaven/press-releases/2011/pdf/nh041311_1.pdf	The U.S. Attorney's Office for the District of Connecticut filed a civil complaint against 13 "John Doe" defendants on the grounds of wire fraud, bank fraud, and illegal interception of electronic communications.	http://www.fbi.gov/news/stories/2011/april/botnet_041411/botnet_041411 http://www.fbi.gov/newhaven/press-releases/2011/nh041311.htm http://www.htnp.com/easthampton/2011/04/13/fbi-cracks-international-bot-network-that-has-infected-more-than-2-million-computers/

A
APPENDIX
TABLE A

Cybercrime Related to Financial Institutions with Direct Costs

Continued from last page

Cybercrime Related to Financial Institutions with Direct Cost							
Cyber Crime Case	**Affected Jurisdictions**	**Target(s) of attack**	**Damages Incurred**	**Responding Entity**	**Indictment(s)**	**Case information** (legal provision that case was charged under)	**Resources**
Gauss (2012)	**Origin:** Unknown **Target:** Lebanon and Middle Eastern Financial Institutions.	Mainly Lebanese banks (Blombank, ByblosBank and Credit Libanais) but also Citibank and paypal costumers	Gauss covertly collects banking credentials, web browsing history and passwords, and detailed technical information about the computer that could assist further attacks.	Kapersky Labs detected the Gauss virus.	N/A	N/A	http://www.telegraph.co.uk/technology/internet-security/9466718/Cyber-espionage-virus-targets-Lebanese-banks.html?mobile=basic
Dyre Banking Trojan (aka Dyreza, Dyzap, and Dyranges) (2014)	**Origin:** Eastern Europe or Russia **Target:** Mainly U.S. and UK	Targeted customers of over 1,000 banks and companies worldwide. Consumers in English-speaking countries were at highest risk, particularly those in the U.S. and UK.	Theft of credentials (identity informational like date of birth as well as PIN codes and credit card details)	The Dell SecureWorks Counter Threat Unit (CTU) research team discovered the Virus in June 2014.	N/A	N/A	http://www.secureworks.com/cyber-threat-intelligence/threats/dyre-banking-trojan/ http://www.symantec.com/connect/blogs/dyre-emerges-main-financial-trojan-threat

A
APPENDIX
TABLE A

Cybercrime Related to Financial Institutions with Direct Costs

Continued from last page

Cybercrime Related to Financial Institutions with Direct Cost							
Cyber Crime Case	**Affected Jurisdictions**	**Target(s) of attack**	**Damages Incurred**	**Responding Entity**	**Indictment(s)**	**Case information** (legal provision that case was charged under)	**Resources**
Dridex Banking Trojan (July 2014- Oct. 2014)	**Origin:** **Target:** United States, UK, Taiwan, Neherlands, Canada, Australia, Belgium, Israel, Germany, Norway, Spain, other.	Personal computers- The trojan takes personal information such as usernames and passwords with the end goal of hacking bank accounts and stealing funds. Also focused on small- and medium-sized organisations.	The National Crime Agency says that "up to" £20m was lost to the hackers, and the FBI says that a first $10m was lost domestically. $1m was stolen from a school district in Pennsylvania and successfully transferred. Over $3.5m was stolen from Penneco Oil in the course of three separate attacks.	Governmental entities, International entities, and private industry.	N/A	N/A	http://researchcenter.paloaltonetworks.com/2014/10/dridex-banking-trojan-distributed-word-documents/ http://www.bankinfosecurity.com/dridex-banking-trojan-worldwide-threat-a-7557/op-1 http://www.theguardian.com/technology/2015/oct/14/what-is-dridex-how-can-i-stay-safe

A
APPENDIX
TABLE A

Cybercrime Related to Financial Institutions with Direct Costs

Continued from last page

Cybercrime Related to Financial Institutions with Direct Cost							
Cyber Crime Case	**Affected Jurisdictions**	**Target(s) of attack**	**Damages Incurred**	**Responding Entity**	**Indictment(s)**	**Case information** (legal provision that case was charged under)	**Resources**
Gozi Bank Malware (2005-2010)	**Origin:** Russia, Latvia, Romania **Target:** U.S.	Financial Institutions	tens of millions	FBI led investigation beginning in 2010. Law Enforcement and Intelligence authorities in latvia, Romania, Moldova, the Netherlands, Germany, Finland, Switzerland, the U.K. and the U.S.	http://www.justice.gov/usao/nys/pressreleases/January13/GoziVirusDocuments/Kuzmin,%20Nikita%20Complaint.pdf http://www.justice.gov/usao/nys/pressreleases/January13/GoziVirusDocuments/Calovskis,%20Deniss%20S4%20Indictment.pdf http://www.justice.gov/usao/nys/pressreleases/January13/GoziVirusDocuments/Paunescu,%20Mihai%20Ionut%20Indictment.pdf	The creator of the Gozi malware along with two co-conspirators were charged for infecting more than a million computers worldwide in order to steal banking and other credentials from tens of thousands of victims.	http://www.huffingtonpost.com/2013/01/23/gozi-virus-fbi_n_2535282.html

A
APPENDIX
TABLE A

Cybercrime Related to Financial Institutions with Direct Costs

Continued from last page

Cybercrime Related to Financial Institutions with Direct Cost							
Cyber Crime Case	**Affected Jurisdictions**	**Target(s) of attack**	**Damages Incurred**	**Responding Entity**	**Indictment(s)**	**Case information** (legal provision that case was charged under)	**Resources**
US v Liberty Reserve et al (costa rican-based digital currency exchange) (Liberty Reserve was indicted on Tuesday May 28th 2013)	**Origin:** Laundering funds internationally **Target:** U.S. and others	N/A (was a money laundering case)	Estimated to have laundered $6 billion	The United States Secret Service, the Internal Revenue Service-Criminal Investigation, and the U.S. Immigration and Customs Enforcement's Homeland Security Investigations, which worked together in this case as part of the Global Illicit Financial Team. The Judicial Investigation Organization in Costa Rica, Interpol, the National High Tech Crime Unit in the Netherlands, the Spanish National Police, Financial and Economic Crime Unit, the Cyber Crime Unit at the Swedish National Bureau of Investigation, and the Swiss Federal Prosecutor's Office. The case is being prosecuted by the Department of Justice's Asset Forfeiture and Money Laundering Section and the Department of Justice's Office of International Affairs and Computer Crime and Intellectual Property Section (more specifically the Office's Complex Frauds and Cybercrime Unit and Money Laundering and Asset Forfeiture Unit)	http://www.justice.gov/usao/nys/pressreleases/May13/LibertyReservePR/Liberty%20Reserve,%20et%20al.%20Redacted%20AUSA%20Appln%20with%20exhibits.pdf	1 count conspiracy to commit money laundering, 1 count conspiracy to operate unlicensed money transmitting business, and 1 count operation of an unlicensed money transmitting business.	http://www.justice.gov/usao/nys/pressreleases/May13/LibertyReserveetalDocuments.php http://www.reuters.com/article/2013/05/28/net-us-cybercrime-libertyreserve-charges-idUSBRE94R0KQ20130528 https://www.justice.gov/usao-sdny/pr/founder-liberty-reserve-arthur-budovsky-pleads-guilty-manhattan-federal-court

A
APPENDIX
TABLE A

Cybercrime Related to Financial Institutions with Direct Costs

Continued from last page

Cybercrime Related to Financial Institutions with Direct Cost							
Cyber Crime Case	**Affected Jurisdictions**	**Target(s) of attack**	**Damages Incurred**	**Responding Entity**	**Indictment(s)**	**Case information** (legal provision that case was charged under)	**Resources**
Unlimited Operation (Oct. 2012 to Apr. 2013)	**Origin:** New York based-cell, but the organization is multinational. **Target:**	First attack targeted a card processor that handled transactions for prepaid mastercard debit cards from the National Bank of Ras Al-Khaimah PSC (RAKBANK). The second attack targeted the same type of cards issued by the Bank of Muscat in Oman.	$45 million USD	The investigation was led by the United States Secret Service with support from the Department of Homeland Security as well as Mastercard, RAKBANK, and the Bank Muscat. Law enforcement authorites in Japan, Canada, Germany, and Romania, and also thanked authorities in the United Arab Emirates, Dominican Republic, Mexico, Italy, Spain, Belgium, France, United Kingdom, Latvia, Estonia, Thailand, and Malaysia also cooperated with the investigation.	http://www.justice.gov/usao/nye/pr/2013/2013may09.html	N/A	https://nakedsecurity.sophos.com/2013/05/10/casher-crew-from-global-cyberheist-busted-in-new-york/
Project Blitzkrieg (Oct. 2012)	**Origin:** Launched from a server in Ukraine. **Target:** U.S.	30 U.S. banks. Credit card unions, federal credit union, genereic banking platforms, investment banks, large national banks, national banks, online payment processors, regional banks and state credit unions. To include Bank of America, Capital One and Suntrust, and investment banks such as American Funds, Ameritrade, eTrade, Fidelity, OptionsExpress, and Schwab.	$5 million USD was stolen by one group in 2008 using this virus.	RSA claimed that they had discovered an operation run by an individual known as vorVzakone	N/A	N/A	http://krebsonsecurity.com/2012/10/project-blitzkrieg-promises-more-aggressive-cyberheists-against-u-s-banks/#more-17096 http://www.mcafee.com/us/resources/white-papers/wp-analyzing-project-blitzkrieg.pdf http://krebsonsecurity.com/2012/12/new-findings-lend-credence-to-project-blitzkrieg/

A
APPENDIX
TABLE A

Cybercrime Related to Financial Institutions with Direct Costs

Continued from last page

Cybercrime Related to Financial Institutions with Direct Cost							
Cyber Crime Case	**Affected Jurisdictions**	**Target(s) of attack**	**Damages Incurred**	**Responding Entity**	**Indictment(s)**	**Case information** (legal provision that case was charged under)	**Resources**
United States v Albert Gonzalez (2009)	**Origin:** U.S. **Target:** U.S.	Large corporate networks with credit card and atm numbers saved within internal servers.	$200 million USD	The investigation was led by the United States Secret Service with support from the Federal Bureau of Investigation.	https://www.justice.gov/opa/pr/alleged-international-hacker-indicted-massive-attack-us-retail-and-banking-networks	19 counts of conspiracy, computer fraud, wire fraud, access device fraud and aggravated identity theft.	https://www.justice.gov/opa/pr/international-hacker-pleads-guilty-massive-hacks-us-retail-networks
Zberp (2014)	**Origin: N/A** **Target:** Mainly in the U.S., U.K. and Australia	Targeting more than 450 financial institutions around the world.	N/A	Discovered and named by security researchers from IBM subsidiary Trusteer.	N/A	N/A	http://securityintelligence.com/new-zberp-trojan-discovered-zeus-zbot-carberp/

A
APPENDIX
TABLE A

Cybercrime Related to Financial Institutions with Indirect Costs

Cybercrime related to Financial Institutions with Indirect Costs							
Cyber Crime Case	**Affected Jurisdictions**	**Target(s) of attack**	**Damages Incurred**	**Responding Entity**	**Indictment(s)**	**Case information** (legal provision that case was charged under)	**Resources**
JPMorgan Chase and 9 other U.S. banks (8/1/2014)	**Origin:** Believed to be from Russia **Target:** U.S.	10 U.S. financial institutions including JPMorgan Chase	Bank Data (mainly coustomer personal data)	**For JP Morgan:** JP Morgan's security team first identified the attack. The U.S. Department of Treasury, the Secret Service and intelligence agencies have been working alonside JP Morgan's security team to locate the source of the attack.	N/A	N/A	http://dealbook.nytimes.com/2014/10/03/hackers-attack-cracked-10-banks-in-major-assault/?_r=0 http://www.symantec.com/connect/app#!/blogs/us-banks-breached-cyberattack-what-bankers-should-do-stay-protected-0 http://www.nytimes.com/2014/08/28/technology/hackers-target-banks-including-jpmorgan.html?_r=2 https://www.bloomberg.com/news/videos/b/0e6c09e9-c79c-4e3f-8cd4-6903468411ce http://www.nytimes.com/interactive/2014/10/03/business/dealbook/jpmorgan-documents.html
Nasdaq (Feb. 5, 2011)	**Origin:** N/A **Target:** U.S.	Web-based app callled directors desk, where companies can share info, may have been hacked. Has 5,000 users.	Unclear what was taken but the portion of the Nasdaq which handles trades was not hacked.	Intially investigated by the United States FBI and NSA. Follow-up investigations were carried out by the the National Cybersecurity and Communications Integration Center (NCCIC).	N/A	N/A	http://www.wsj.com/articles/SB10001424052748704843304576126370179332758 http://www.nytimes.com/2011/02/06/business/06nasdaq.html

A
APPENDIX
TABLE A

Cybercrime Related to Financial Institutions with Indirect Costs

Continued from last page

Cybercrime related to Financial Institutions with Indirect Costs							
Cyber Crime Case	**Affected Jurisdictions**	**Target(s) of attack**	**Damages Incurred**	**Responding Entity**	**Indictment(s)**	**Case information** (legal provision that case was charged under)	**Resources**
Target (Nov. 27- Dec. 15, 2013)	**Origin:** N/A **Target:** U.S.	Customer Data	40 million customers' credit card information, and 70 million others	Federal Law Enforcement officials notified Target of the breach on December 12, 2013. Company investigators worked to uncover what happened.	N/A	N/A	http://bits.blogs.nytimes.com/2014/11/06/home-depot-says-hackers-also-stole-email-addresses/?ref=topics http://dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues/ http://money.cnn.com/2013/12/22/news/companies/target-credit-card-hack/ http://www.bloomberg.com/news/articles/2014-03-13/target-missed-warnings-in-epic-hack-of-credit-card-data
Home Depot (April, 2014)	**Origin:** N/A **Target:** U.S.	Customer Data	53 million customer email addresses, payment card details for millions, (56 million in totoal affected)	N/A	N/A	N/A	http://bits.blogs.nytimes.com/2014/11/06/home-depot-says-hackers-also-stole-email-addresses/?ref=topics http://dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues/ http://www.wsj.com/articles/home-depot-hackers-used-password-stolen-from-vendor-1415309282
T.J. Maxx (July 2005-December 2006)	**Origin:** N/A **Target:** U.S.	Customer Data	Data for 90 million customers	N/A	N/A	N/A	http://www.nytimes.com/2013/12/20/technology/target-stolen-shopper-data.html http://www.washingtonpost.com/wp-dyn/content/article/2007/09/25/AR2007092500836.html

A
APPENDIX
TABLE A

Cybercrime Related to Financial Institutions with Indirect Costs

Continued from last page

Cybercrime related to Financial Institutions with Indirect Costs							
Cyber Crime Case	**Affected Jurisdictions**	**Target(s) of attack**	**Damages Incurred**	**Responding Entity**	**Indictment(s)**	**Case information** (legal provision that case was charged under)	**Resources**
Sony & Qriocity (April-17-19, 2011)	**Origin:** U.S., U.K. and Ireland **Target:** U.S.	Sensitive customer information	Sensitive information for 77 million customers (personal information and perhaps credit card numbers)	FBI	https://www.wired.com/wp-content/uploads/2014/05/Monsegur.pdf	N/A	http://money.cnn.com/gallery/technology/security/2013/12/19/biggest-credit-card-hacks/5.html
Neiman Marcus	**Origin:** Russia **Target:** U.S.	Sensitive customer information	1 million credit card information stolen	N/A	N/A	N/A	http://www.bloomberg.com/news/articles/2014-04-07/neiman-marcus-breach-linked-to-russians-who-eluded-u-s-
Rex Mundi (Jan. 2015) (twiiter account name which announced the hacking event)	**Origin:** N/A **Target:** Swiss bank BCGE	Banque Cantonale de Geneve (confidential client information)	Hacked system and stole 30,000 emails of clients from the bank and attempted to extort 10,000 euros in exchange for not publishing the information.	N/A	N/A	N/A	http://www.reuters.com/article/2015/01/09/us-bc-geneve-hacker-idUSKBN0KI1MK20150109

A
APPENDIX
TABLE A

Cybercrime Related to Financial Institutions with Indirect Costs

Continued from last page

Cybercrime related to Financial Institutions with Indirect Costs							
Cyber Crime Case	**Affected Jurisdictions**	**Target(s) of attack**	**Damages Incurred**	**Responding Entity**	**Indictment(s)**	**Case information** (legal provision that case was charged under)	**Resources**
com.ll (Summer 2014 (hack announced by cheetah mobile on June 27th))	**Origin:** N/A **Target:** Korea	Kookmin, Nong Hyup, Shinhan, Hana N, Woori, Busan, and the Korean Federation of Community Credit Cooperatives	Costumer bank log in information, bank account information, phone numbers, device IDs, and contact lists	South Korean Police	N/A	N/A	http://www.securityweek.com/new-android-malware-targets-banking-apps-phone-information-fireeye https://www.fireeye.com/blog/threat-research/2014/07/the-service-you-cant-refuse-a-secluded-hijackrat.html http://www.securityweek.com/fake-android-apps-target-south-korean-bank-customers
Dump Memory Grab (2013)	**Origin:** Russian Federation **Target:** U.S.	Major U.S. banks (chase, capital one, citibank, and union bank of california)	harvest info from credit and debit cards	N/A	N/A	N/A	http://www.securityweek.com/exclusive-new-malware-targeting-pos-systems-atms-hits-major-us-banks
vSkimmer (Feb. 2013-)	**Origin:** Circulating on criminal forums out of Russia **Target:** Multinational	Designed capture credit card data from systems running Windows that host payment processing software.	Credit card information	The vskimmer malware was first detected by McAfee's sensor network.	N/A	N/A	http://www.securityweek.com/exclusive-new-malware-targeting-pos-systems-atms-hits-major-us-banks http://www.securityweek.com/vskimmer-botnet-targeting-payment-card-terminals-connected-windows http://www.computerworld.com/article/2495732/cybercrime-hacking/researchers-uncover-vskimmer-malware-targeting-point-of-sale-systems.html

Cybercrime Related to Financial Institutions with Indirect Costs

Continued from last page

Cybercrime related to Financial Institutions with Indirect Costs							
Cyber Crime Case	**Affected Jurisdictions**	**Target(s) of attack**	**Damages Incurred**	**Responding Entity**	**Indictment(s)**	**Case information** (legal provision that case was charged under)	**Resources**
Dexter (Sept.-Dec. 2012)	**Origin:** N/A **Target:** Multinational	42% of infections in North America. Mostly big-name retail, hotels, restaurants, private parking providers, and eateries.	Credit card information. Loss of 80,00 credit cards from Subway restaurants in 2012	N/A	N/A	N/A	http://www.securityweek.com/exclusive-new-malware-targeting-pos-systems-atms-hits-major-us-banks http://www.securityweek.com/new-malware-targets-point-sale-systems-just-time-holiday-rush http://www.securityweek.com/vskimmer-botnet-targeting-payment-card-terminals-connected-windows
Airline Fraud Scheme (11/1/2014)	**Origin:** Multinational **Target:** 60 airlines in over 45 countries. Also greatly impacted the banking and travel sectors as well as airlnes.	60 airlines in over 45 countries	Nearly $1 billion from the airline industry alone	Europol in The Hague, Netherlands; INTERPOL through its General Secretariat in Lyon, France and the INTERPOL Global Complex for Innovation (IGCI) in Singapore; and AMERIPOL in Bogota, Colombia. More than 60 airlines and 45 countries were involved in the activity, which took place at some 80 airports across the world. The International Air Transport Association (IATA) also took part in the investigation.	118 individuals were arrested	Defendants from various jurisdictions were charged for crimes related to credit card fraud.	https://www.europol.europa.eu/content/118-arrested-global-action-against-online-fraudsters-airline-sector https://www.unodc.org/cld/case-law-doc/cybercrimecrimetype/xxx/operation_global_action_against_online_fraudsters_in_the_airline_sector.html?&tmpl=cyb http://www.interpol.int/News-and-media/News/2014/N2014-228

A
APPENDIX
TABLE A

Major Cybercrime by Individuals/Groups

Major Cybercrime by Individuals/Groups							
Cyber Crime Syndicate	**Affected Jurisdictions**	**Target(s) of attack**	**Damages Incurred**	**Responding Entity**	**Indictment(s)**	**Case information**	**Resources**
Russian Cybercrime Syndicate	**Origin:** N/A **Target:** U.S.	Heartland Payment Systems 2007 (130 million credit cards), Hannaford Brothers Co 2007 (4.2 million card numbers), Carrefour S.A. 2007 (2 million card numbers), Commidea Ltd. 2008, (30 million card numbers), Euronet 2010 (2 million card numbers), Visa, Inc 2011 (800,000 card numbers), Discover Financial Services (500,000 diners card numbers). Also hacked into NASDAQ, 7-Eleven, JetBlue, JCPenny, Wet Seal, Dexia, Dow Jones, & Ingenicard.	More than 160 million credit card numbers from U.S. retailers, banks and card processors.	The U.S. Secret Service, Criminal Investigations, led the investigation. The U.S. also collaborated with the New Jersey U.S. Attorney's Office Criminal Division, The Department of Justice's Computer Crime and Intellectual Section as well as with the Dutch Ministry of Security and Justice and the National High Tech Crime Unit of the Dutch National Police.	U.S. v. Drinkman, Kalinin, Kotov, Rytikov, & Smilianets http://www.justice.gov/usao/nj/Press/files/pdffiles/2013/Drinkman,%20Vladimir%20%20et%20al.,%20Indictment.pdf	http://www.justice.gov/usao/nj/Press/files/Drinkman,%20Vladimir%20et%20al.%20Indictment%20News%20Release.html	http://krebsonsecurity.com/tag/aleksandr-kalinin/ http://www.justice.gov/usao/nj/Press/files/Drinkman,%20Vladimir%20et%20al.%20Indictment%20News%20Release.html https://nakedsecurity.sophos.com/2010/03/25/tjx-hacker-jail-20-years-stealing-40-million-credit-cards/ http://www.nytimes.com/2013/12/20/technology/target-stolen-shopper-data.html http://www.bloomberg.com/bw/stories/2009-07-06/lessons-from-the-data-breach-at-heartlandbusinessweek-business-news-stock-market-and-financial-advice

A
APPENDIX
TABLE A

Major Cybercrime by Individuals/Groups

Continued from last page

Major Cybercrime by Individuals/Groups							
Cyber Crime Syndicate	**Affected Jurisdictions**	**Target(s) of attack**	**Damages Incurred**	**Responding Entity**	**Indictment(s)**	**Case information**	**Resources**
Sonya Martin	**Origin:** Chicago, Illinois, U.S.A. **Target:** Multinational	Personal Bank Accounts with ATM withdrawal capabilities.	$9 million was stolen from over 2,100 ATMs in at least 280 cities worldwide, including cities in the United States, Russia, Ukraine, Estonia, Italy, Hong Kong, Japan, and Canada. The event took place in less than 12 hours on Nov. 8, 2008.	The U.S. Federal Bureau of Investigation led the investigation with assistance provided by numerous domestic and international law enforcement partners. WorldPay reported the crime and substantially assisted in the investigation. Case was prosecuted by the Department of Justice Computer Crime and Intellectual Property Section with assistance from the Department of Justice Office of International Affairs.	N/A	http://www.fbi.gov/atlanta/press-releases/2012/sentencing-in-major-international-cyber-crime-prosecution	https://nakedsecurity.sophos.com/2012/08/28/prison-atm-worldpay/
Chinese-Run Cybercrime Network	**Origin:** China via Kenya **Target:** Kenya	"The group had been preparing to "raid the country's communication systems" and had equipment capable of infiltrating bank accounts, Kenya's M-Pesa mobile banking system and ATM machines."retrieved from http://www.bbc.com/news/world-africa-30327412	N/A (Attack foiled)	Kenyan Police	N/A	N/A	http://www.nation.co.ke/news/77-Chinese-held-in-cyber-bust/-/1056/2543786/-/t5vf43/-/index.html http://www.theguardian.com/world/2014/dec/05/kenya-chinese-nationals-cybercrime-nairobi http://www.newsweek.com/77-chinese-nationals-arrested-kenya-cybercrimes-289539

Major Cybercrime by Individuals/Groups

Continued from last page

Major Cybercrime by Individuals/Groups							
Cyber Crime Syndicate	**Affected Jurisdictions**	**Target(s) of attack**	**Damages Incurred**	**Responding Entity**	**Indictment(s)**	**Case information**	**Resources**
Evgeniy Bogachev	**Origin:** Western District of Pennsylvania **Target:** U.S. and elsewhere	Financial Institutions	$100 million stolen	Besides the United States, law enforcement from the Australian Federal Police; the National Police of the Netherlands National High Tech Crime Unit; European Cybercrime Centre (EC3); Germany's Bundeskriminalamt; France's Police Judiciare; Italy's Polizia Postale e delle Comunicazioni; Japan's National Police Agency; Luxembourg's Police Grand Ducale; New Zealand Police; the Royal Canadian Mounted Police; Ukraine's Ministry of Internal Affairs – Division for Combating Cyber Crime; and the United Kingdom's National Crime Agency participated in the operation. The Defense Criminal Investigative Service of the U.S. Department of Defense also participated in the investigation. Invaluable technical assistance was provided by Dell SecureWorks and CrowdStrike. Numerous other companies also provided assistance, including facilitating efforts by victims to remediate the damage to their computers inflicted by Gameover Zeus. These companies include Microsoft Corporation, Abuse.ch, Afilias, F-Secure, Level 3 Communications, McAfee, Neustar, Shadowserver, Anubis Networks, Symantec, Heimdal Security, Sophos and Trend Micro.	http://www.justice.gov/sites/default/files/opa/legacy/2014/06/02/pittsburgh-indictment.pdf https://web.archive.org/web/20160926103934/https://www.justice.gov/opa/documents-and-resources-june-2-2014-announcement	1 count conspiracy, 1 count of wire fraud, 1 count of computer fraud, 9 counts of bank fraud, and 2 count of money laundering.	http://www.justice.gov/sites/default/files/opa/legacy/2014/06/02/pittsburgh-indictment.pdf http://www.bbc.com/news/world-us-canada-31614819 http://www.justice.gov/opa/pr/us-leads-multi-national-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware

Major Cybercrime by Individuals/Groups

Continued from last page

Major Cybercrime by Individuals/Groups							
Cyber Crime Syndicate	**Affected Jurisdictions**	**Target(s) of attack**	**Damages Incurred**	**Responding Entity**	**Indictment(s)**	**Case information**	**Resources**
African Cyber Criminal Enterprise (ACCE)	**Origin:** Commonly Nigeria **Target:** U.S.	More than 85 companies and universities in the U.S. Approxiamtely 400 actual or attempted incidents targeting 250 vendors.	Retail goods. Approxiamtely $5 million lost so far. After the fraud is discovered, the retailer is forced to absorb the financial losses.	FBI	N/A	N/A	http://www.fbi.gov/washingtondc/press-releases/2014/african-cyber-criminal-enterprise-members-using-school-impersonation-scheme-to-defraud-retailers http://www.fbi.gov/news/stories/2014/april/understanding-school-impersonation-fraud https://www.ic3.gov/media/2014/140904.aspx https://www.fbi.gov/news/stories/purchase-order-scam-leaves-a-trail-of-victims
Online Marketplace Fraud	**Origin:** Romania and other European countries **Target:** U.S.	Users of online marketplace and auction websites such as ebay.com, cars.com, autotrader.com, and cycletrader.com.	Funds from consumers using online marketplace websites. Attacks resulted in potentially million dollar losses to U.S. victims.	FBI	http://www.justice.gov/usao/nye/pr/2013/doc/Popescu.Signed%20Indictment%20(12%20CR%20785).pdf	1 count of conspiracy to commit wire fraud, money laundering and passport fraud to traffic in counterfeit service marks, 7 counts of wire fraud, 2 counts of wire fraud, 4 counts of wire fraud, 1 count of passport fraud, 1 count of passport fraud, 1 count of trafficking in counterfeit service marks, 1 count of money laundering, 1 count of money laundering, 1 count of money laundering, 1 count of money laundering, 1 count fo money laundering, 1 count of money laundering.	http://www.state.gov/j/inl/tocrewards/c64997.htm http://www.state.gov/j/inl/tocrewards/c64996.htm

A
APPENDIX
TABLE A

Major Cybercrime by Individuals/Groups

Continued from last page

Major Cybercrime by Individuals/Groups							
Cyber Crime Syndicate	**Affected Jurisdictions**	**Target(s) of attack**	**Damages Incurred**	**Responding Entity**	**Indictment(s)**	**Case information**	**Resources**
People's Liberation Army (PLA) Unit 61398 (Defendants Charged on May 19, 2014)	**Origin:** China **Target:** U.S., Western District of Pennsylvania.	American commercial enterprises (nuclear, metal and solar firms). Alcoa Inc, Allegheny Technologies Inc, United States Steel Corp, Toshiba Corp unit Westinghouse Electric Co, the U.S. subsidiaries of SolarWorld AG, and a steel workers' union were among the targeted institutions.	Information stolen from commerical enterprises to be used by competitors in China. Information such as trade secrets.	The investigation was led by the U.S. FBI. The case is being prosecuted by the U.S. Department of Justice's National Security Division Counterespionage Section and the U.S. Attorney's Office for the Western District of Pennsylvania.	**Indictment:** http://www.justice.gov/iso/opa/resources/512201451913235846 1949.pdf	1 count of conspiracy to commit computer fraud and abuse, 8 counts of computer fraud and abuse, 14 counts of damaging a computer, 6 counts of aggravated identity theft, 1 count of economic espionage, and 1 count of theft of trade secret.	http://www.reuters.com/article/2014/05/20/us-cybercrime-usa-china-unit-idUSBREA4J08M20140520 https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor
Roman Valerevich Seleznev (Oct. 2, 2009 - Feb. 22, 2011)	**Origin: Servers were located in Russia, Ukraine, and multiple servers in the U.S. such as McLean Virginia.** **Target:** Westerm District of Washinton and elsewhere.	Defraud various financial insitutions including Boeing Employee's Credit Union, Chase Bank, Capital One, Citibank, and Keybank.	Stole and sold credit card numbers. At least $1.7 million in losses to banks and credit card companies.	The U.S. Secret Service Electronic Crimes Task Force (includes detectives from the Seattle Police Department)	**Indictment:** http://krebsonsecurity.com/wp-content/uploads/2014/07/Seleznev-Indictment-CR11-0070RAJ-1.pdf	5 counts of Bank fraud, 8 counts of intentional damage to a protected computer, 8 counts of obtaining information from a protected computer, 1 coutn of possession of fifteen or more unauthorized access devices, 2 counts of trafficking in unauthorized access devices, and 5 counts of aggravated identity theft.	http://www.capitolhillseattle.com/2014/07/russian-hacker-arrested-in-2010-broadway-grill-data-breach http://www.justice.gov/usao-wdwa/pr/alleged-russian-cyber-criminal-now-charged-40-count-superseding-indictment

A
APPENDIX
TABLE A

Major Cybercrime by Individuals/Groups

Continued from last page

Major Cybercrime by Individuals/Groups							
Cyber Crime Syndicate	**Affected Jurisdictions**	**Target(s) of attack**	**Damages Incurred**	**Responding Entity**	**Indictment(s)**	**Case information**	**Resources**
Alexsey Belan (Jan. 2012- Apr. 2013)	**Origin:** Multinational **Target:** Nevada and San Francisco, U.S.	E-commerce companies.	Stole, exported and sold user databases from e-commerce companies.	U.S. Federal and state authorities.	N/A	In Nevada, charged with obtaining information from a protected computer; possession of fifteen or more unauthorized access devices; and aggravated identity theft. In San Francisco, was charged with two fraud counts and two counts of aggravated identity theft.	http://rt.com/news/fbi-wanted-list-russian-340/ https://www.fbi.gov/wanted/cyber/alexsey-belan/view
Alexandr Sergeyevich Bobnev (June 2007 -August 2007)	**Origin:** Russian Federation **Target:** U.S.	Scheme utilized the accounts of major provider of investment services.	Attempted to steal and launder funds from investment service accounts. Wired or attempted to wire $350,000	FBI	Southern District of New York indicted him on Nov. 26, 2008	1 count of conspiracy to commit wire fraud and 1 count of conspiracy to commit money laundering	http://www.fbi.gov/wanted/cyber/alexandr-sergeyevich-bobnev/view

A
APPENDIX
TABLE A

Major Cybercrime by Individuals/Groups

Continued from last page

Major Cybercrime by Individuals/Groups							
Cyber Crime Syndicate	**Affected Jurisdictions**	**Target(s) of attack**	**Damages Incurred**	**Responding Entity**	**Indictment(s)**	**Case information**	**Resources**
Yahoo! Inc. Email Hack	**Origin:** Russia and Canada **Target:** Everywhere	500 million email addresses	$350 million	US Justice Department, FBI, Canada	N/A	A Canadian, Karim Baratov, is accused in a massive hack of Yahoo emails (500 million emails) in 2014. Baratov was arrested under the Extradition Act after U.S. authorities indicted him and three others — two of them allegedly officers of Russia's Federal Security Service — for computer hacking, economic espionage and other crimes.	https://www.justice.gov/opa/press-release/file/948201/download
Guccifer Case	**Origin:** Romania **Target:** Hilary Clinton (USA)	Hilary Clinton's private email domain	N/A	FBI, DSS, and Secret Service	https://assets.documentcloud.org/documents/1197719/lazar-indictment.pdf	Marcel Lazar, a Romanian hacker nicknamed "Guccifer" who helped expose the existence of a private email domain Hillary Clinton used when she was U.S. secretary of state was sentenced to 52 months in prison by a federal court in Alexandria, Virginia after pleading builty in May 2017 to including unauthorized access to a protected computer and aggravated identity theft after being extradited from Romania.	https://www.justice.gov/usao-edva/pr/romanian-hacker-guccifer-sentenced-prison

A
APPENDIX
TABLE A

Major Cybercrime by Individuals/Groups

Continued from last page

Major Cybercrime by Individuals/Groups							
Cyber Crime Syndicate	**Affected Jurisdictions**	**Target(s) of attack**	**Damages Incurred**	**Responding Entity**	**Indictment(s)**	**Case information**	**Resources**
The Yanbian Gang	**Origin:** the Yanbian Prefecture in Jilin, China. **Target:** South Korea	Targeted mobile banking customers of at least five banks in South Korea since 201. These banks included B Kookmin Bank, NH Bank, Hana Bank, Shinhan Bank, and Woori Bank.	The Yanbian cybergang is thought to have stolen millions from at least five korean banks.	Yanbian gang hack was first documented and detailed by Trend Micro Mobile Threat Team.	N/A	N/A	http://www.securityweek.com/cyber-gang-steals-millions-mobile-banking-customers-south-korea http://www.securityweek.com/chinas-cybercrime-marketplace-boomed-2013-trend-micro http://www.securityweek.com/16-million-mobile-devices-infected-malware-2014-alcatel-lucent http://www.securityweek.com/inside-chinas-market-mobile-cybercrime http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-the-south-korean-fake-banking-app-scam.pdf
New York Money Mules Online Bank Fraud Scheme'	**Origin:** Based in Eastern Europe but had money mule network in U.S. **Target:** U.S.	Bank accounts belonging primarily to small businesses and municipalities.	Stole more than $3 million	FBI agents and agents of the Secret Service, ICE, and the State Department's Diplomatic Security Service carried out arrests in this multi-defendant case targeting overseas computer hackers.	37 people were charges in 21 cases. "An arrest warrant was issued for Semenov in the Southern District of New York on September 29, 2010, after he was charged with conspiracy to commit bank fraud; conspiracy to possess false identification documents; and false use of passport."	"Semenov... was charged with conspiracy to commit bank fraud; conspiracy to possess false identification documents; and false use of passport" retrieved from http://www.fbi.gov/wanted/cyber/artem-semenov/view	http://www.wired.com/2010/09/zeus-botnet-ring/ http://www.rferl.org/content/In_US_Cybercrime_Case_Track_Record_Indicates_Russia_Willing_To_Cooperate/2185564.html

Cybercrime Targeting Non-Financial Institutions and Financial Institutions

Cybercrime Targeting Non-Financial Institutions and Financial Institutions							
Cyber Crime Case	**Affected Jurisdictions**	**Target(s) of attack**	**Damages Incurred**	**Responding Entity**	**Court Documents**	**Case info.** (legal provision that case was charged under)	**Resources**
DDoS Attack against National (Central) Election Commission Homepage (2011, October, 26)	**Origin:** Korea **Target:** Korea	National (Central) Election Commission Homepage, Finding the polling place Function	Not related to this case	1. National Police Agency in cooperation with National Cyber Security Center and 2. Seoul Central District Prosecutors' Office Special Investigation Team in cooperation with Korea Internet Security Agency did investigation.	Korean Supreme Court Decision 2012 Do 16086 Decided March 28, 2013, available at: http://glaw.scourt.go.kr/	**Legal provisions:** N/A. **Potentially relevant provisions:** 1. Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.; Articles 48, Paragraph 3; 71, Subparagraph 10; 2. Act on the Protection of Information and Communications Infrastructure, Articles 12; 28; 3. Public Officials Election Act, Article 237, Paragraph 1	1. KSPO Press Release: http://www.spo.go.kr/seoul/notice/notice/notice01.jsp?mode=view&board_no=116&article_no=523931 2. Chosun Ilbo (English Edition), News: http://english.chosun.com/site/data/html_dir/2011/10/27/2011102701142.html

A
APPENDIX
TABLE A

Cybercrime Targeting Non-Financial Institutions and Financial Institutions

Continued from last page

Cybercrime Targeting Non-Financial Institutions and Financial Institutions							
Cyber Crime Case	**Affected Jurisdictions**	**Target(s) of attack**	**Damages Incurred**	**Responding Entity**	**Court Documents**	**Case info.** (legal provision that case was charged under)	**Resources**
Prosecution v. Baksa Timea and Others (Criminal activities started in 2002)	**Origin:** Hungary **Target:** Hungary	Mainly: Copyright-protected content	N/A Relevant Info: Seizedmoney-48,000,000 HUF The criminal organization engaged in money laundering (proceeds of illegal activities) assisted by Ukrainian nationals (According to law enforcement info-761,000,000 HUF between 2007 and 2009).	Hungarian law enforcement searched 5 server rooms, seized 48 servers . In response to Hungarian authorities request sent out to Romanian authorities via INTERPOL channels, the information on the death of the leader of the criminal orgs was obtained.	N/A	N/A	UNODC, Cybercrime Repository: http://www.unodc.org/cld/case-law-doc/cybercrimecrimetype/hun/prosecution_vs._baksa_timea_and_others.html
Credit Card Data Theft in Romania (2015)	**Origin:** Romania **Target:** Touristic areas in Croatia and Turkey	Credit card data of wealthy tourists in Croatia and Turkey	N/A	During the house searches executed at the premises of the defendants were found skimming devices. A computer search revealed that the defendants used software able to read the magnetic tracks of credit cards.	N/A	**Legal Provisions:** 1. Law No. 39 of 2003 on preventing and combating organized crime, Aricle.7, Paragraph 1 (Initiation or constitution of an organized criminal group). 2. Law No. 365 of 2002 on electronic commerce, Article 25 (Possession of equipment with a view to forging electronic means of payment).	UNODC Cybercrime Repository http://www.unodc.org/cld/case-law-doc/cybercrimecrimetype/rou/credit_card_data_theft_in_romania.html

Cybercrime Targeting Non-Financial Institutions and Financial Institutions

Continued from last page

Cybercrime Targeting Non-Financial Institutions and Financial Institutions							
Cyber Crime Case	**Affected Jurisdictions**	**Target(s) of attack**	**Damages Incurred**	**Responding Entity**	**Court Documents**	**Case info.** (legal provision that case was charged under)	**Resources**
Online Storage Companies, Aiding and Abetting Violation of Copyright Act, etc. (Not specified, but the investigation result was released to the press on April 20, 2012)	**Origin:** Republic of Korea **Target:** Republic of Korea	(Copyright-Protected) Work	Not specified, but the proceeds of illegal activities through leaving the (copyright-protected) work (illegally uploaded) on the online storage sites : 1,140,000,000 Won (according to the Seoul Central District Prosecutors' Office info)	Seoul Central District Prosecutors' Office	N/A	Specific provisions are not provided: Possibly relevant provisions: (1) Aid, Abet Violation of Copyright Act Copyright Act, Article 136, Paragraph 1; Copyright Act, Article 140, Sub-paragraph 1 1; Criminal Act, Article 32, Paragraph 1; (2) Violation of Copyright Act: Article 136, Paragraph 1;' Copyright Act; Article 140, Sub-paragraph 1	KSPO Press Release: http://www.spo.go.kr/seoul/notice/notice01.jsp?mode=view&board_no=116&article_no=533012
Apprehension of Voice Phishing Organization in the Republic of Korea -Voice Phishing against Low Credit Individuals in the Dorm of Fake Loans (From November, 2011 to April, 2012)	**Origin:** Republic of Korea **Target:** Republic of Korea	Individuals with poor credit ratings and who need loan services	Three billion four hundred million Won (KRW 3,400, 000, 000)	Seoul Central District Prosecutors' Office	N/A	Specific provisions: NA. Possibly relevant provisions: 1, Criminal Act, Article 347 (Fraud); 2. Act on the Aggravated Punishment, etc. of Specific Economic Crimes, Article 3, Paragraph 1, Subparagraph 2 (Aggravated Punishment of Specific Property Crime)	KSPO Press Release http://www.spo.go.kr/seoul/notice/notice01.jsp?mode=view&board_no=116&article_no=533736

A
APPENDIX
TABLE A

Cybercrime Targeting Non-Financial Institutions and Financial Institutions

Continued from last page

Cybercrime Targeting Non-Financial Institutions and Financial Institutions							
Cyber Crime Case	**Affected Jurisdictions**	**Target(s) of attack**	**Damages Incurred**	**Responding Entity**	**Court Documents**	**Case info.** (legal provision that case was charged under)	**Resources**
Fraudulent eBay Auctions in Romania (Between 2006 and 2009)	**Origin:** Romania **Target:** Spain, Italy, France, New Zealand, Denmark, Sweden, Germany, Austria, the United States, Canada and Switzerland	users of eBay auctions located in different countries	Fraudsters stole the Euro equivalent of more than $1 million.	Romanian authorities[Romanian Directorate for Investigating Organized Crime and Terrorism (DIICOT)], in conjunction with U.S. law enforcement (in partnership with the FBI and U.S. Secret Service from the U.S. Embassy in Bucharest), arrested alleged offenders.	N/A	N/A	1. SC Magazine News: http://www.scmagazine.com/romanian-police-fbi-break-up-70-strong-ebay-fraud-ring/article/167554/ 2. UNODC Cybercrime Repository: http://www.unodc.org/cld/case-law-doc/cybercrimecrimetype/rou/fraudulent_ebay_auctions_in_romania.html
Operation Exposure (Date of arrest: February, 2012)	**Origin:** The servers used for the purposes of administration of some of the secure communication channels used by Anonymous were hosted by companies located in Czech Republic and Bulgaria, although they were remotely controlled from Spain. **Target:** Unclear. However, among its victims are governmental agencies of the U.S., Israel, Tunisia and Uganda.	1. Governmental agencies of the U.S., Israel, Tunisia and Uganda websites; 2. child pornography websites; 3.copyright protection institutions; religious entities; and private corporations, including PayPal, MasterCard, Visa and Sony websites	N/A	With the support of Europol, law enforcement agencies of the involved countries carried out the investigation (**1.** Simultaneous arrests; **2.** Search and seizure; **3.** Server disruptions and **4.** Expedited preservation of computer data)	N/A	Specific legal provision are not available. According to UNODC Cybercrime Repository, the suspects were charged with illegal interference, breach of privacy and disclosure of confidential information.	1. UNODC Cybercrime Repository: http://www.unodc.org/cld/case-law-doc/cybercrimecrimetype/esp/operation_exposure.html 2. EUROPOL Press Release: https://www.europol.europa.eu/newsroom/news/hacktivists-arrested-in-spain

Cybercrime Targeting Non-Financial Institutions and Financial Institutions

Continued from last page

Cybercrime Targeting Non-Financial Institutions and Financial Institutions							
Cyber Crime Case	**Affected Jurisdictions**	**Target(s) of attack**	**Damages Incurred**	**Responding Entity**	**Court Documents**	**Case info.** (legal provision that case was charged under)	**Resources**
Violation of Criminal Act, Act on Promotion of Information and Communications Network Utilization and Information Protection, etc., and Game Industry Promotion Act (2009-2013)	**Origin:** Korea **Target:** Korea	Divulged personal Information of another person	1. Proceeds from acquiring game items (jointly with defendant 1): KRW 125, 678, 400 2. Proceeds from the sale of game items (1) Jointly with defendant 1: KRW 405, 471, 229 (2) Solely by defendant 2: KRW 1,901, 266, 177	Prosecutors, Police, Judges	[1] Korean Supreme Court Decision 2014 Do 8838 Decided Nov. 13, 2014; [2] Seoul Central District Court Decision 2012 No 323 Decided Jun. 26, 2014, and [3] Seoul Central District Court Decision 2013 Go Dan 4451, 2013 Go Dan 4488 (Consolidation) Decided Jan. 15, 2014, available at: http://glaw.scourt.go.kr/wsjo/intesrch/sjo022.do	1. Criminal Act, Art. 347-2; 2. Game Industry Promotion Act, Arts. 32, Para. 7, and 44, Para 1, Subpara 2. [and its Enforcement Decree, Art. 18-3., Para. 3, Subpara c. and Former Enforcement Decree (prior to the Amendment No. 23863, June 19, 2012) Art. 18-3, Subpara. 3.; 3. Act on Promotion of Information and Communications Network Utilization and Information Protection, etc., Arts. 28-2, Para 2. and 71, Subpara 6.	Korean Court Decisions on this case, available at: http://glaw.scourt.go.kr/wsjo/intesrch/sjo022.do
Prosecution of People Who Stole Personal Information and Data, Forged National Identity Cards, Illegally Opened Cell Phone Accounts (February, 2011 to August, 2013)	**Origin:** Republic of Korea **Target:** Republic of Korea	Stolen Personal Information/Data	N/A	Police officers and prosecutors, in collaboration with mobile phone companies (private sector) and sharing investigation know-how between police officers and prosecutors, carried out investigation.	N/A	Violation of 1. Personal Information Protection Act, 2. Criminal Act, 3. Act on the Aggravated Punishment, etc. of Specific Economic Crimes 4. Act on Promotion of Information and Communications Network Utilization and Information Protection, etc., and 5. Radio Wave Act	KSPO Press Release: http://www.spo.go.kr/seoul/notice/notice01.jsp?mode=view&board_no=116&article_no=585659

Cybercrime Targeting Non-Financial Institutions and Financial Institutions

Continued from last page

Cybercrime Targeting Non-Financial Institutions and Financial Institutions							
Cyber Crime Case	**Affected Jurisdictions**	**Target(s) of attack**	**Damages Incurred**	**Responding Entity**	**Court Documents**	**Case info.** (legal provision that case was charged under)	**Resources**
Arrest of an organization based in China which asked hacking and selling/supplying or purchasing personal information/data (From May, 2012 to February, 2014)	**Origin:** China, Korea **Target:** Korea	Personal Information/data	N/A	Seoul Central District Prosecutors' Office	N/A	Specific legal provisions are not provided. Attackers 1, 2, 5, 8 and 9 were charged with violation of Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. according to KSPO press release.	KSPO Press Release: http://www.spo.go.kr/seoul/notice/notice01.jsp?mode=view&board_no=116&article_no=572591
Credit Card Companies, leakage of customer information in the Republic of Korea (From May, 2012 to December, 2013)	**Origin:** Republic of Korea **Target:** Republic of Korea	Customer information (Personal Information held by credit card firms) including financial data	The customer data of at least 26 million (26,000,000) people was illegally collected.	Changwon District Prosecutors' Office	N/A	Specific law and legal provision are not available. However, posisbly relevant law: Violation of Personal Information Protection Act	1. KSPO Press Release: http://www.spo.go.kr/spo/notice/press/press.jsp?mode=view&board_no=2&article_no=567739 2. ZDNet, Security, Newsletter http://www.zdnet.com/article/south-korean-credit-card-firms-suspended-over-data-breach/

A
APPENDIX
TABLE A

Cybercrime Targeting Non-Financial Institutions and Financial Institutions

Continued from last page

Cybercrime Targeting Non-Financial Institutions and Financial Institutions							
Cyber Crime Case	**Affected Jurisdictions**	**Target(s) of attack**	**Damages Incurred**	**Responding Entity**	**Court Documents**	**Case info.** (legal provision that case was charged under)	**Resources**
Apprehension of members of a criminal organization that committed international financial scams (From January, 2011 to July, 2012 (1 year and 7 months))	**Origin:** Republic of Korea (""Korea"") **Target:** (Commercial Banks located in) U.S.	USD $11, 000,000 [KRW 12,200,000,000] [Additional issue: Money laundering]	Commercial Banks (located in U.S.)	In cooperation with (or "Through mutual assistance") Federal Bureau of Investigation (FBI), Korean National Police Agency (KNPA) identified this organization and arrested its members (Nigerians and Korean) located in Korea during the period of time ranging from July 19, 2012 to October 8, 2012.	Indictment(s)/Court Decision(s): Not publicly available online as of June 2, 2015	According to KNPA press release, legal provisions applicable to this case is 1. Article 347, Paragraph 1 (Fraud); 2. Article 231 (Counterfeit or Alteration of Private Document, etc.); 3. Article 234 (Uttering of Falsified Private Document, etc.) of the Criminal Act.	1. Korean National Police Agency (KNPA) Press Release: http://www.spo.go.kr/spo/notice/press/press.jsp?mode=view&board_no=2&article_no=567739 2. Hankook Ilbo News News, http://www.koreatimes.com/article/836700
The organization that illegally won (online) construction bids of Nara Jangteo, Korea's online e-procurement system through hacking a computer system was busted (From May 2011 to October 2012)	**Origin:** Korea **Target:** Korea	Computer system of Nara Jangteo, Korea's online e-procurement system, which is operated by the Public Procurement Service (PPS)	By manipulating the lowest bidding price, the companies won 77 construction bids, worth a total of 110 billion won.	Seoul Central District Prosecutors' Office	N/A	All relevant legal provisions are not provided. However, possibly relevant legal provisions: 1. Criminal Act, Article 347-2 (Fraud by Use of Computer, etc.) 2. Criminal Act, Article 315 (Interference with Auction or Bidding) 3. Act on the Protection of Information and Communications Infrastructure, Articles 12; 28	1. Korea Joongang Daily, Social Affairs, News: http://koreajoongangdaily.joins.com/news/article/article.aspx?aid=2981472 2. KSPO Press Release: http://www.spo.go.kr/seoul/notice/notice/notice01.jsp?mode=view&board_no=116&article_no=565540

A
APPENDIX
TABLE A

Cybercrime Targeting Non-Financial Institutions and Financial Institutions

Continued from last page

Cybercrime Targeting Non-Financial Institutions and Financial Institutions							
Cyber Crime Case	**Affected Jurisdictions**	**Target(s) of attack**	**Damages Incurred**	**Responding Entity**	**Court Documents**	**Case info.** (legal provision that case was charged under)	**Resources**
Operation Imperium (Date of incident: Unclear Date of arrest: September 30, 2014)	**Origin:** European countries **Target:** 1. Obtaining credit card info in EU (e.g. Italy, France, Spain, Germany, and Turkey), 2. Withdrawing cash: outside EU (e.g. in Peru and the Philippines).	1. Credit/financial card data; 2. (ATM) Payment system	N/A	Bulgarian and Spanish law enforcement and judicial agencies together with Europol's European Cybercrime Centre (EC3) did a joint operation. 26 arrests & 40 house searches in Bulgaria five arrests and two house searches in Spain.	N/A	N/A, however, according to UNODC Cybercrime Repository, 31 members of an organized criminal group were arrested for ATM skimming, electronic payment fraud, forgery of documents and other crimes (possibly breach of privacy or data protection measures).	1. UNODC Cybercrime Repository: http://www.unodc.org/cld/case-law-doc/cybercrimecrimetype/bgr/2014/operation_imperium.html 2. EUROPOL Press Release: https://www.europol.europa.eu/content/31-arrests-operation-against-bulgarian-organised-crime-network
Pletnyov Operation (July 2005 - November 2006)	**Origin:** Not explicitly state jurisdictional origin. According to UNODC Cybercrime Repository, victims funds were wired to Hungary, Slovakia, the Czech Republic and Poland controlled by co-conspirators. **Target:** Attackers targeted U.S. and other nationals with online fraud	Targeted U.S. and other nationals who were using E-bay or other web sites subject to defendants' cyber attacks in issue	N/A	This investigation was conducted by the FBI-Hungarian National Bureau of Investigation (HNBI) Organized Crime Task Force located in Hungary. (Bilateral and multilateral cooperation)	N/A. However, according to UNODC Cybercrime Repository, the indictment expressly charged the defendants with conspiracy to launder money and conspiracy to commit wire fraud.	N/A. However, according to UNODC Cybercrime Repository, all of the defendants were charged and adjudicated in federal court in the District of Columbia. (Thus, it is presumed that U.S. laws were applied to this case).	UNODC Cybercrime Repository: http://www.unodc.org/cld/case-law-doc/cybercrimecrimetype/usa/pletnyov_operation.html

Cybercrime Targeting Non-Financial Institutions and Financial Institutions

Continued from last page

Cybercrime Targeting Non-Financial Institutions and Financial Institutions							
Cyber Crime Case	**Affected Jurisdictions**	**Target(s) of attack**	**Damages Incurred**	**Responding Entity**	**Court Documents**	**Case info.** (legal provision that case was charged under)	**Resources**
Operation against Remote access Trojans (Date of arrest: around November 2014 according to EUROPOL Press Release)	**Origin:** Involved countries: several EU countries According to UNODC Cybercrime Repository, the international operation – led by France - resulted in the arrest of 15 individuals in Estonia, France, Romania, Latvia, Italy and the U.K. **Target:** Involved countries: several EU countries According to UNODC Cybercrime Repository, the international operation – led by France - resulted in the arrest of 15 individuals in Estonia, France, Romania, Latvia, Italy and the U.K.	Operation of remote access Trojans	N/A	According to EUROPOL's press release, the operation was led by France- working with Europol's European Cybercrime Centre (EC3) and the involved European countries (Estonia, France, Romania, Latvia, Italy, and U.K.) authorities.	N/A	N/A. However, according to UNODC Cybercrime Repository, the use of remote access in Europe is punished by a number of offences, including illegal access to computer data, breach of privacy and illegal interception.	1. UNODC Cybercrime Repository: http://www.unodc.org/cld/case-law-doc/cybercrimecrimetype/fra/2014/operation_against_remote_access_trojans.html 2. EUROPOL's Press Release: https://www.europol.europa.eu/content/users-remote-access-trojans-arrested-eu-cybercrime-operation

Cybercrime Targeting Non-Financial Institutions and Financial Institutions

Continued from last page

Cybercrime Targeting Non-Financial Institutions and Financial Institutions							
Cyber Crime Case	**Affected Jurisdictions**	**Target(s) of attack**	**Damages Incurred**	**Responding Entity**	**Court Documents**	**Case info.** (legal provision that case was charged under)	**Resources**
Operation Stop Intrusion	**Origin:** Jurisdictional origin: Not explicitly provided. [Countries involved in the operation: 1. Romania, 2. Malaysia, and 3. Italy] **Target:** Jurisdictional target: Not explicitly provided. [Countries involved in the operation: 1. Romania, 2. Malaysia, and 3. Italy]	Employees of the Italian Ministry of Foreign Affairs and other civil servants' credentials and access restricted information	N/A	International cooperation (including INTERPOL) through the 24/7 Network as well as formal cooperation. The 24/7 Network is intended to offer computer crime investigators a fast and reliable channel to request preservation of computer evidence. Further evidence was later obtained through formal mutual legal assistance procedures.	N/A	N/A	UNODC Cybercrime Repository: http://www.unodc.org/cld/case-law-doc/cybercrimecrimetype/ita/operation_stop_intrusion.html

Cybercrime Targeting Non-Financial Institutions and Financial Institutions

Continued from last page

Cybercrime Targeting Non-Financial Institutions and Financial Institutions							
Cyber Crime Case	**Affected Jurisdictions**	**Target(s) of attack**	**Damages Incurred**	**Responding Entity**	**Court Documents**	**Case info.** (legal provision that case was charged under)	**Resources**
Investigation on "DIABLO" and "CODER"	**Origin:** N/A, but possibly Morocco (Moroccan police identified three alleged perpetrators, two Moroccans and one Turk after being informed by their American counterparts) **Target:** Not provided in UNODC Cybercrime Repository, but possibly includes U.S. Besides, a suspect used the stolen data to withdraw large sums of money from bank accounts of people living in Russia.	a cyber attack on several multinational groups (With specific regard to one of suspects: stolen credit card data and passwords from multinational companies' websites)	According to the victims, this virus caused more than USD $ 5 million in losses.	Moroccan police was informed by their American counterparts of a cyber attack. The investigation by the Moroccan police led to the identification of three alleged perpetrators, two Moroccans and one Turk. This case is considered to be the first cybercrime case in Morocco. Judicial and police international cooperation proved to be key in order to identify the suspects.	N/A [According to UNODC Cybercrime Repository, no information on the proceedings is available.]	According to UNODC Cybercrime Repository, the relevant offences are codified in the Moroccan Penal Code, in particular Articles 607-11 and 607-3.	UNODC Cybercrime Repository: http://www.unodc.org/cld/case-law-doc/cybercrimecrimetype/mar/investigation_on_diablo_and_coder.html

Cybercrime Targeting Non-Financial Institutions and Financial Institutions

Continued from last page

Cybercrime Targeting Non-Financial Institutions and Financial Institutions							
Cyber Crime Case	**Affected Jurisdictions**	**Target(s) of attack**	**Damages Incurred**	**Responding Entity**	**Court Documents**	**Case info.** (legal provision that case was charged under)	**Resources**
U.S. vs. 18 defendants **[Joint U.S. - South Africa Operation]** (2001-2014)	**Origin:** Counts 1, 2, and 3: In Harrison County, in the Southern Division of the Southern District of Mississippi and elsewhere. Defendants were resided & arrested in U.S., Canada, and South Africa. **Target:** Not specified. However, according to U.S. Immigration and Customs Enforcement (ICE) news, investigators have so far identified hundreds of victims to this financial fraud scam in the U.S.	1. Personal identification information (PII) 2. Credit card/ bank data; and Information on credit card/bank accounts, etc. 3. United States Postal Service (U.S.P.S.) shipping labels 4. Government funds, etc.	According to U.S. ICE news, this financial fraud scam has resulted in the loss of millions of U.S. dollars.	1. U.S. ICE 2. U.S. Homeland Security Investigations (HSI) 3. South African Police Service's Directorate for Priority Crime Investigation 4. South Africa's Crime Intelligence 5. INTERPOL 6. South Africa Tactical Response Team 7. South Africa Department of Home Affairs – Immigration	**Indictment:** http://www.ice.gov/doclib/news/releases/2014/140521pretoria.pdf	1. Count 1 : 18 U.S.C. § 1341, 1343, 1344 & 1349 2. Count 2: 18 U.S.C. §1028 (a)(7); 1029 (a)(3); 1029(a)(5); 641; & 371 3. Count 3: 18 U.S.C. § 1341	1. UNODC Cybercrime Repository: http://www.unodc.org/cld/case-law-doc/cybercrimecrimetype/usa/joint_us_-_south_africa_operation.html 2. U.S. Immigration and Customs Enforcement (ICE), News: http://www.ice.gov/news/releases/cyber-financial-fraud-investigation-nets-numerous-arrests-south-africa-canada-us

Cybercrime Targeting Non-Financial Institutions and Financial Institutions

Continued from last page

Cybercrime Targeting Non-Financial Institutions and Financial Institutions							
Cyber Crime Case	**Affected Jurisdictions**	**Target(s) of attack**	**Damages Incurred**	**Responding Entity**	**Court Documents**	**Case info.** (legal provision that case was charged under)	**Resources**
U.S. v. Kilbride (2003)	**Origin:** Defendants operated of their business overseas, running it through Ganymede Marketing ("Ganymede"), a Mauritian company, and using servers located in the Netherlands. **Target:** Unclear, but including individuals located in U.S. [U.S. government called 8 witnesses from various parts of the country who had complained to the Federal Trade Commission about defendants' emails.]	Individuals who received defendants' emails	N/A	U.S. Ninth Circuit Court of Appeals: The court affirmed the defendants' convictions and sentences and recognized that there was a clerical error with regard to counts 1-3 (the CAN-SPAM Act offences) and remanded.	**Information on court decision:** http://www.nyls.edu/wp-content/uploads/sites/141/2013/08/584-F.3d-1240-US-v.-Kilbride.pdf	1. Computer Fraud and Abuse Act, 18 U.S.C. § 1037(a)(3), § 1037(a)(3) and (a)(4); 2. 18 U.S.C. § 1462; 3. 18 U.S.C. § 1465; 4. 18 U.S.C. § 1956; and =5. 18 U.S.C. § 2257.[The court recognized there was a clerical error with regard to acts relating to the CAN-SPAM Act (15. U.S.C.) offenses and remanded.]	UNODC Cybercrime Repository: http://www.unodc.org/cld/case-law-doc/cybercrimecrimetype/usa/2009/us_v_kilbride.html

Cybercrime Targeting Non-Financial Institutions and Financial Institutions

Continued from last page

Cybercrime Targeting Non-Financial Institutions and Financial Institutions							
Cyber Crime Case	**Affected Jurisdictions**	**Target(s) of attack**	**Damages Incurred**	**Responding Entity**	**Court Documents**	**Case info.** (legal provision that case was charged under)	**Resources**
Operation: In Our Sites (IOS) Transatlantic V [the transnational operation – called 'In Our Sites (IOS) Transatlantic V'] (Date of incident: Unrelated to this operation , Date of seizure of Intellectual Property (IP) infringing websites: since November 2012 (according to UNODC Cybercrime Repository))	**Origin:** Jurisdictional Origin: Unrelated to this operation. (Countries involved in this operation: several EU countries and U.S. according to UNODC Cybercrime Repository) **Target:** Unrelated to this operation (Countries involved in this operation: several EU countries and U.S. according to UNODC Cybercrime Repository)	Patent holders of infringed websites and the customers who purchased counterfeit goods from the infringed websites	(Computer-related or online) Infringement of IP Rights by selling, purchasing (or trafficking) counterfeit products on websites by infringing IP rights' holders	1. EUROPOL and U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) together with 25 law enforcement agencies from 19 countries carried out this investigation. 2. Trademarks holders reported several infringing websites to EUROPOL and U.S. National Intellectual Property Rights Coordination Center (IPR Center), which alerted the competent national authorities	N/A	N/A	1. UNODC Cybercrime Repository: http://www.unodc.org/cld/case-law-doc/cybercrimecrimetype/xxx/operation_in_our_sites_ios_transatlantic_v.html 2. EUROPOL Press Release: https://www.europol.europa.eu/content/292-internet-domain-names-seized-selling-counterfeit-products

Cybercrime Targeting Non-Financial Institutions and Financial Institutions

Continued from last page

Cybercrime Targeting Non-Financial Institutions and Financial Institutions							
Cyber Crime Case	**Affected Jurisdictions**	**Target(s) of attack**	**Damages Incurred**	**Responding Entity**	**Court Documents**	**Case info.** (legal provision that case was charged under)	**Resources**
Operation Strikeback (Date of incident: unrelated to this operation, Date of launch of this operation: late in 2013)	**Origin:** Unrelated to this operation (Countries involved in this operation: Philippines, U.K., U.S., Australia, Indonesia, Malaysia, Republic of Korea according to UNODC Cybercrime Repository) **Target:** Unrelated to this operation (Countries involved in this operation: Philippines, U.K., U.S., Australia, Indonesia, Malaysia, Republic of Korea according to UNODC Cybercrime Repository)	Victims of 'sextortion'	Online sexual exploitation (online sextortion cases)	INTERPOL Digital Crime Centre (IDCC) launched the operation in cooperation with Police Scotland, the US Immigration and Customs Enforcement (ICE), the Philippines Department of Justice Office of Cybercrime, the U.K.'s National Crime Agency CEOP Command, the Hong Kong Police Force and the Singapore Police Force. The investigators identified (1) victims in a number of jurisdictions, including Indonesia, the Philippines, the U.K. and the U.S. and (2) potential victims in Australia, Hong Kong, Korea, Malaysia and Singapore.	N/A	N/A	1. UNODC Cybercrime Repository: http://www.unodc.org/cld/case-law-doc/cybercrimecrimetype/phl/operation_strikeback.html 2. INTERPOL Press Release: http://www.interpol.int/News-and-media/News/2014/N2014-075 3. Timeline of Operation Strikeback combating 'sextortion' http://www.unodc.org/res/cld/case-law-doc/cybercrimecrimetype/phl/operation_strikeback_html/2014-075-Timeline-of-Operation-Strikeback.pdf

Cybercrime Targeting Non-Financial Institutions and Financial Institutions

Continued from last page

Cybercrime Targeting Non-Financial Institutions and Financial Institutions							
Cyber Crime Case	**Affected Jurisdictions**	**Target(s) of attack**	**Damages Incurred**	**Responding Entity**	**Court Documents**	**Case info.** (legal provision that case was charged under)	**Resources**
Facebook, Inc. v. Jeremy Fisher, etc. (Since November 2008)	**Origin:** (Name of the State, U.S. where the defendants resided or located) D1, D4: New York; D2, D5, D6 California; D3, D7: Colorado **Target:** (Facebook servers located in) California	Facebook servers (located in California)	N/A	According to UNODC case Info, the U.S. District Court for the Northern District of California San Jose Division issued an Order Granting Motion for a Temporary Restraining Order (TRO) upon request of Facebook. [Further details to be checked by review of the Complaint, TRO, and order granting plaintiff's motion for declaratory judgment.]	TRO: https://cases.justia.com/federal/district-courts/california/candce/5:2009cv05842/222386/21/0.pdf?ts=1377125623 Order granting plaintiff's motion for declaratory judgment: http://www.plainsite.org/dockets/download.html?id=24299386&z=e2682a55	1. Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM), 15 U.S.C. § 7701, etseq,; 2. Computer Fraud and Abuse Act, 18 U.S.C. § 1030; 3. California Business and Professions Code,§ 22948, The California Anti-Phishing Act of 2005; 4. California Comprehensive Computer Data Access and Fraud Act, California Penal Code § 502.	UNODC, Cybercrime Repository: http://www.unodc.org/cld/case-law-doc/cybercrimecrimetype/usa/2009/facebook_inc_v_jeremy_fisher.html
Microsoft (MS) v. ZeroAccess Botnet operators [Operation: Disruption of the ZeroAccess botnet] (2013)	**Origin:** Texas and the Western District of Texas, U.S. **Target:** 1. ZeroAccess Infected Computers: located in U.S. and Europe; 2. Infected computers relied on servers located at 18 IP addresses and 49 Internet domains maintained by defendants at hosting companies in Germany, Latvia, Switzerland, Luxembourg, and the Netherlands.	(1) Infecting computers of individuals: Computers of individuals (2) Online advertising fraud (browser hijacking and click fraud): MS, and its advertiser , and/or customers	Infecting more than 2 million computers, specifically targeting search results on Google, Bing and Yahoo search engines, and is estimated to cost online advertisers $2.7 million each month.	MS Digital Crimes Unit disrupted a botnet in collaboration with (1) EUROPOL's European Cybercrime Centre (EC3); (2) law enforcement cybercrime units from Germany, Latvia, Luxembourg, Switzerland and the Netherlands; (3) FBI; and (4) leaders in the technology industry, including A10 Networks Inc.	Complaint: http://botnetlegalnotice.com/zeroaccess/files/Cmplt.pdf Temporary Restraining Order(s): 1) Jason Lyons, http://botnetlegalnotice.com/zeroaccess/files/Decl_Lyons.pdf 2) David Anselmi, http://botnetlegalnotice.com/zeroaccess/files/Decl_Anselmi.pdf	1. Computer Fraud and Abuse Act, 18 U.S.C. § 1030 2. Electronic Communications Privacy Act, 18 U.S.C. § 2701 3. Trademark Infringement Under the Lanham Act, 15 U.S.C.§ 1114 et. Seq. 4. False Designation of Origin Under the Lanham Act, 15 U.S.C. § 1125(a) 5. Trademark Dilution Under the Lanham Act, 15. U.S.C. § 1125 (C)	1. UNODC Cybercrime Repository: http://www.unodc.org/cld/case-law-doc/cybercrimecrimetype/xxx/2013/operation_disruption_of_the_zeroaccess_botnet.html 2. Microsoft News Center: http://news.microsoft.com/2013/12/05/microsoft-the-fbi-europol-and-industry-partners-disrupt-the-notorious-zeroaccess-botnet/ 3. EUROPOL Press Release https://www.europol.europa.eu/content/notorious-botnet-infecting-2-million-computers-disrupted

Cybercrime Targeting Non-Financial Institutions and Financial Institutions

Continued from last page

Cybercrime Targeting Non-Financial Institutions and Financial Institutions							
Cyber Crime Case	**Affected Jurisdictions**	**Target(s) of attack**	**Damages Incurred**	**Responding Entity**	**Court Documents**	**Case info.** (legal provision that case was charged under)	**Resources**
U.S. v. Blake Benthall **[Operation Onymous (an operation launched by law enforcement officers and prosecutors in 16 European countries and U.S., coordinated with EUROPOL in Nov. 2014)]** (1. Providing a platform for illicit trafficking in goods and services (fraudulent identification docs, drugs, hacking services): Nov. 2013 to Oct. 2014 2. Money laundering: Dec. 2013 to Oct. 2014)	**Origin:** Southern District of New York, U.S. and elsewhere **Target:** Not specified in a complaint, but possibly global, including Southern District of New York, U.S. and elsewhere (A Tor network is a worldwide network)	1. Computer-related illicit trafficking in goods and services (in drugs, fraudulent identification documents and computer-hacking services) 2. Computer-related money laundering	Amount of damages: N/A. According to the FBI, as of September 2014, Silk Road 2.0 was generating sales of at least approximately $8 million per month and approximately 150,000 active users.	According to FBI , 1. FBI with help from the following, among others, 2. New York State Police, 3. Department of Justice's Computer Crime and Intellectual Property Section, 4. Drug Enforcement Administration; and 5. law enforcement authorities of France, Germany, Lithuania, the Netherlands, and the U.K. According to UNODC, 6. service providers and 7. EUROPOL	Complaint: http://www.justice.gov/usao/nys/pressreleases/November14/BlakeBenthallArrestPR/Benthall,%20Blake%20Complaint.pdf.	1. Narcotics trafficking conspiracy: 21 (Title 21). U.S.C. (United States Code), § (Section) 846; 2. Conspiracy to commit and aid and abet computer hacking: 18. U.S.C. § 1030(b); 3. Conspiracy to transfer fraudulent identification documents: 18. U.S.C. § 1028 (f); and 4. Money laundering conspiracy: 18. U.S.C. § 1956 (h)	1. UNODC Cybercrime Repository, http://www.unodc.org/cld/case-law-doc/cybercrimecrimetype/xxx/operation_onymous.html 2. EUROPOL Press Release, https://www.europol.europa.eu/content/global-action-against-dark-markets-tor-network 3. FBI Press Release, https://www.fbi.gov/contact-us/field-offices/newyork/news/press-releases/operator-of-silk-road-2.0-website-charged-in-manhattan-federal-court

Cybercrime Targeting Non-Financial Institutions and Financial Institutions

Continued from last page

Cybercrime Targeting Non-Financial Institutions and Financial Institutions							
Cyber Crime Case	**Affected Jurisdictions**	**Target(s) of attack**	**Damages Incurred**	**Responding Entity**	**Court Documents**	**Case info.** (legal provision that case was charged under)	**Resources**
UEJF and LICRA v Yahoo! Inc and Yahoo France (2000)	**Court's Location:** France **Place where defendants are incorporated:** Yahoo, France: France; Yahoo! Inc.: USA	N/A	Computer-related acts involving racism and xenophobia	N/A	N/A	**Court Decision:** The court ordered Yahoo! Inc. to take all the measures necessary to dissuade and prevent access to auctions for Nazi memorabilia and content supporting Nazism. The court ordered Yahoo, France to warn users that, should Yahoo's search results include content prohibited under French law, they shall refrain from accessing such content to avoid incurring legal sanctions. **Legal Provision:** French Criminal Code, Article R645-1 which prohibits to "wear or exhibit" in public uniforms, insignias and emblems which "recall those used" by (i) an organization declared illegal in application of Art. 9 of the Nuremberg Charter, or (ii) a person found guilty of crimes against humanity.	UNODC Cybercrime Repository**:** http://www.unodc.org/cld/case-law-doc/cybercrimecrimetype/fra/2000/uejf_and_licra_v_yahoo_inc_and_yahoo_france.html

Cybercrime Targeting Non-Financial Institutions and Financial Institutions

Continued from last page

Cybercrime Targeting Non-Financial Institutions and Financial Institutions							
Cyber Crime Case	**Affected Jurisdictions**	**Target(s) of attack**	**Damages Incurred**	**Responding Entity**	**Court Documents**	**Case info.** (legal provision that case was charged under)	**Resources**
Yahoo! Inc. v UEJF and LICRA (1. District Court, Proceedings 1 and 2: 2001, 2. Court of Appeals for the Ninth Circuit, Proceeding 3: 2004; Proceeding 4: 2006; and 3. Supreme Court, Proceeding 5: 2006)	**Court location:** U.S. **Location where defendants are incorporated:** 1. UJEF (Union of French Jewish Students): French non-profit organization 2. LICRA (International League against Racism and Anti-Semitism): French organization	N/A	Computer-related acts involving racism and xenophobia [Allowing users to post Nazi paraphernalia and Third Reich memorabilia, in violation of Article R645-1 of French Criminal Code on Yahoo! Inc.run-auction websites.]	N/A	N/A	**U.S. Supreme Court's Decision:** Proceeding 5 (2006) The Supreme Court denied LICRA's request to issue an order to review the judgment (certiorari), http://www.unodc.org/res/cld/case-law-doc/cybercrimecrimetype/usa/2006/yahoo_inc_v_uejf_and_licra__html/Supreme_Court_Certiorari.pdf **Issue 1. legitimacy of limitations to freedom of expression:** The need for a balance between freedom of expression and prohibition of online illegal speech has been addressed in different ways under different jurisdictions. **Issue 2. Extraterritorial applicability of domestic laws:** Transnational character of online communications challenges the concept of traditional jurisdiction. Asserting jurisdiction over website operators cause concerns over applicability of laws of the country where their websites are accessible.	UNODC Cybercrime Repository: http://www.unodc.org/cld/case-law-doc/cybercrimecrimetype/usa/2006/yahoo_inc_v_uejf_and_licra_.html

A
APPENDIX
TABLE A

Other Forms of Cybercrime

Other Forms of Cybercrime							
Cyber Crime Case	**Affected Jurisdictions**	**Target(s) of attack**	**Damages Incurred**	**Responding Entity**	**Court Documents**	**Case Information**	**Resources**
Flame and Stuxnet	**Origin:** U.S. & Israel **Target:** Iran, Lebanon, Syria, Sudan and Israeli occupied territories	Intelligence and destroys capacity	N/A	N/A	N/A	N/A	http://rt.com/news/flame-stuxnet-kaspersky-iran-607/ http://www.wired.com/2012/05/flame/
Operation Ghost Click (2007-Oct. 2011)	**Origin:** Estonia **Target:** U.S.	Over 4 million computers were infected in more than 100 countries. In the U.S., 500,000 computers were infected including those used by individuals, as well as computers housed in businesses and government entities such as NASA.	By rerouting internet traffic to websites which allowed for the perpetrators to be paid, the operation generated $14 million in illegitimate income.	The U.S. FBI, NASA OIG, and the Estonian Police and Border Guard Board led the investigation. The National High Tech Crime Unit of the Dutch National Police Agency. The FBI and NASA OIG received assistance from multiple domestic and international private sector partners, including Georgia Tech University, Internet Systems Consortium, Mandiant, National Cyber-Forensics and Training Alliance, Neustar, Spamhaus, Team Cymru, Trend Micro, University of Alabama at Birmingham and members of an ad hoc group of subject matter experts known as the DNS Changer Working Group (DCWG)	https://www.fbi.gov/newyork/press-releases/2011/manhattan-u.s.-attorney-charges-seven-individuals-for-engineering-sophisticated-internet-fraud-scheme-that-infected-millions-of-computers-worldwide-and-manipulated-internet-advertising-business	N/A	http://www.fbi.gov/news/stories/2011/november/malware_110911 https://www.fbi.gov/newyork/press-releases/2011/manhattan-u.s.-attorney-charges-seven-individuals-for-engineering-sophisticated-internet-fraud-scheme-that-infected-millions-of-computers-worldwide-and-manipulated-internet-advertising-business

A
APPENDIX
TABLE A

Other Forms of Cybercrime

Continued from last page

Other Forms of Cybercrime							
Cyber Crime Case	**Affected Jurisdictions**	**Target(s) of attack**	**Damages Incurred**	**Responding Entity**	**Court Documents**	**Case Information**	**Resources**
Morpho Cyber Espionage (2012-present)	**Origin:** N/A **Target:** U.S., Europe, and Canada	High profile technology, internet, commodities, and pharmaceutical companies.	confidential information and intellectual property	Detection by individual companies and private sector entities such as Semantec.	N/A	N/A	http://www.computerweekly.com/news/4500249597/Symantec-uncovers-Morpho-cyber-espionage-operation
Pawn Storm (2014)	**Origin:** N/A **Target:** U.S., Europe, and Pakistan	Military, diplomatic and defence industry	Data	Researchers at Trend Micro uncovered the scheme.	N/A	N/A	http://www.computerweekly.com/news/2240233415/Researchers-uncover-sophisticated-cyber-espionage-campaign
State of Tamil Nadu vs. Suhas Katti (2/1/2004)	**Origin:** India **Target:** India	A known family friend who refused to marry Suhas Katti	Obscene, defamatory and annoying messages in a Yahoo message group	Police responded by tracing the accused to Mumbai and arresting him following a camplaint made by the victim.	N/A	"The accused is found guilty of offences under section 469, 509 IPC and 67 of IT Act 2000 and the accused is convicted and is sentenced for the offence to undergo RI for 2 years under 469 IPC and to pay fine of Rs.500/-and for the offence u/s 509 IPC sentenced to undergo 1 year Simple imprisonment and to pay fine of Rs.500/- and for the offence u/s 67 of IT Act 2000 to undergo RI for 2 years and to pay fine of Rs.4000/- All sentences to run concurrently."	http://lawmantra.co.in/tamil-nadu-v-suhas-katti-2004-case-related-to-the-posting-of-obscene-messages-on-the-internet/

A
APPENDIX
TABLE A

Other Forms of Cybercrime

Continued from last page

Other Forms of Cybercrime							
Cyber Crime Case	**Affected Jurisdictions**	**Target(s) of attack**	**Damages Incurred**	**Responding Entity**	**Court Documents**	**Case Information**	**Resources**
National Association of Software and Service Companies vs Ajay Sood & others (3/1/2005)	**Origin:** India **Target:** India	Software and Service Companies	N/A	Delhi HC issued judgement in the lawsuit	https://indiankanoon.org/doc/1804384/	"The Delhi HC stated that even though there is no specific legislation in India to penalize phishing, it held phishing to be an illegal act by defining it under Indian law as "a misrepresentation made in the course of trade leading to confusion as to the source and origin of the e-mail causing immense harm not only to the consumer but even to the person whose name, identity or password is misused." The court held the act of phishing as passing off and tarnishing the plaintiff's image. The defendants were operating a placement agency involved in head-hunting and recruitment. In order to obtain personal data, which they could use for purposes of headhunting, the defendants composed and sent e-mails to third parties in the name of Nasscom. The high court recognised the trademark rights of the plaintiff and passed an ex-parte adinterim injunction restraining the defendants from using the trade name or any other name deceptively similar to Nasscom. The court further restrained the defendants from holding themselves out as being associates or a part of Nasscom."	http://cyber-law-web.blogspot.com/2009/07/case-study-cyber-law-nasscom-vs-ajay.html

Other Forms of Cybercrime

Continued from last page

Other Forms of Cybercrime							
Cyber Crime Case	**Affected Jurisdictions**	**Target(s) of attack**	**Damages Incurred**	**Responding Entity**	**Court Documents**	**Case Information**	**Resources**
SMC Pneumatics India Pvt. Ltd. v. Jogesh Kwatra (2001)	**Origin:** India **Target:** India	SMC Pnuematics India Pvt. Ltd.	cyber defamation	Court of Delhi	https://indiankanoon.org/doc/31110930/	"After hearing detailed arguments of Counsel for Plaintiff, Hon'ble Judge of the Delhi High Court passed an ex-parte ad interim injunction observing that a prima facie case had been made out by the plaintiff. Consequently, the Delhi High Court restrained the defendant from sending derogatory, defamatory, obscene, vulgar, humiliating and abusive emails either to the plaintiffs or to its sister subsidiaries all over the world including their Managing Directors and their Sales and Marketing departments. Further, Hon'ble Judge also restrained the defendant from publishing, transmitting or causing to be published any information in the actual world as also in cyberspace which is derogatory or defamatory or abusive of the plaintiffs."	http://www.mondaq.com/india/x/218890/Social+Media/Cyber+Defamation+In+Corporate+World

Other Forms of Cybercrime

Continued from last page

Other Forms of Cybercrime							
Cyber Crime Case	**Affected Jurisdictions**	**Target(s) of attack**	**Damages Incurred**	**Responding Entity**	**Court Documents**	**Case Information**	**Resources**
Vyakti Vikas Kendra, India Public Charitable Trust THR Trustee Mahesh Gupta & ORS vs. Jitender Baggaa & ANR. (2013)	**Origin:** India **Target:** India	4 individuals connected to the India Public Trust, His Holiness Sri Sri Ravi Shankar, and Art of Living Teacher.	N/A	Delhi High Court	https://indiankanoon.org/doc/121103864/	Defendant No.2 (D2) is an "intermediary" within the definition of Section 2(1)(w) and Section 79 of the Information Technology Act, 2000. Under Section 79(3)(b) of the IT Act, 2000, D2 is under an obligation to remove unlawful content if it receives actual notice from the affected party of any illegal content being circulated/published through its service. D2 is also bound to comply with Information Technology (Intermediaries Guidelines) Rules 2011. Rule 3(3) of the said rules read with Rule 3(2) requires an intermediary to observe due diligence or publish any information that is grossly harmful, defamatory, libellious, disparaging or otherwise unlawful. Rule 3(4) of the said rule provides obligation of an intermediary to remove such defamatory content within 36 hours from receipt of actual knowledge. The said rule is cited below for easy reference.	https://indiancaselaws.wordpress.com/2013/10/23/vyakti-vikas-kendra-india-public-charitable-trust-thr-trustee-mahesh-gupta-ors-vs-jitender-bagga-anr/

Other Forms of Cybercrime

Continued from last page

Other Forms of Cybercrime							
Cyber Crime Case	**Affected Jurisdictions**	**Target(s) of attack**	**Damages Incurred**	**Responding Entity**	**Court Documents**	**Case Information**	**Resources**
United States v. Ulbricht (2013)	**Origin:** US **Target:** US and everywhere	N/A (was an online black market case)	The operator had over $28.5 million at the time of the seizure	FBI	http://www.nysd.uscourts.gov/cases/show.php?db=special&id=416	Ross Ulbricht, "Dread Pirate Roberts," was convicted and sentenced to life in prison without the possibility of parole for conspiracy and money laundering charges from his role as the operator of the online black market "Silk Road." Using cryptotechnology, the Silk Road facilitated the sale of controlled substances among other things.	https://www.bloomberg.com/news/articles/2017-05-31/silk-road-s-ross-ulbricht-must-serve-life-sentence-court-says

Other Forms of Cybercrime

Continued from last page

Other Forms of Cybercrime							
Cyber Crime Case	**Affected Jurisdictions**	**Target(s) of attack**	**Damages Incurred**	**Responding Entity**	**Court Documents**	**Case Information**	**Resources**
Runescape Case (2012)	**Origin:** Netherlands **Target:** Netherlands	A Runescape player	Virtual items of the victim were transferred to the virtual accounts of the two defendants.	The Dutch Police	https://uitspraken.rechtspraak.nl/#zoekverfijn/ljn=BQ9251&so=Relevance (in Dutch)	On the 31st of January 2012, the Supreme Court of the Netherlands made a ground-breaking decision with implications for the online gaming industry everywhere. It found that items in the online game RuneScape had been stolen from a player. This is revolutionary, as it is the highest national court in the West to rule that taking virtual objects in this way is theft under national criminal law. In 2007, the two defendants used violence and threats of violence to force the victim to log into the game of RuneScape and transferred virtual items and virtual currency from the victims account to their own. The Supreme Court upheld the conviction for theft as defined by the law of the Netherlands.	http://www.virtualpolicy.net/runescape-theft-dutch-supreme-court-decision.html

Other Forms of Cybercrime

Continued from last page

Other Forms of Cybercrime							
Cyber Crime Case	**Affected Jurisdictions**	**Target(s) of attack**	**Damages Incurred**	**Responding Entity**	**Court Documents**	**Case Information**	**Resources**
United States v. Chase (2017)	**Origin:** Naples, Florida (USA) **Target:** US and everywhere	Children	sexual abuse/ exploitation of children	FBI and EUROPOL	N/A	Steven W. Chase, 58, the creator and lead administrator of Playpen, one of the world's largest child sexual abuse websites with more than 150 000 users around the world, was sentenced to 30 years in prison for engaging in a child exploitation enterprise, advertising child pornography, transportation of child pornography and possession of child pornography. This case highlights the use of online forums on anonymous networks to abuse and exploit of innocent children.	https://www.justice.gov/opa/pr/florida-man-sentenced-prison-engaging-child-exploitation-enterprise

A
APPENDIX
TABLE A

Alternate Forms of Cybercrime

Alternate Forms of Cybercrime										
Cyber Crime Case	**Attacker Characteristics**	**Date of Incident**	**Jurisdictional Origin**	**Jurisditional Target**	**Target(s) of attack**	**Methodology of Attack**	**Indictment(s)**	**Responding Entity**	**Case information** (legal provision that case was charged under)	**Resources**
State of Tamil Nadu vs. Suhas Katti	**Suhas Katti:** An idividual who took up harassmentvia the internet against a female target.	Feb-04	India	India	A known family friend who refused to marry Suhas Katti	"Posting of obscene, defamatory, and annoying messages" about the victim in a yahoo message group. The harassment campaign also involved the creation of fake emails and email communications.		Police responded by tracing the accused to Mumbai and arresting him following a camplaint made by the victim.	"The accused is found guilty of offences under section 469, 509 IPC and 67 of IT Act 2000 and the accused is convicted and is sentenced for the offence to undergo RI for 2 years under 469 IPC and to pay fine of Rs.500/- and for the offence u/s 509 IPC sentenced to undergo 1 year Simple imprisonment and to pay fine of Rs.500/- and for the offence u/s 67 of IT Act 2000 to undergo RI for 2 years and to pay fine of Rs.4000/- All sentences to run concurrently."	

A
APPENDIX
TABLE A

Alternate Forms of Cybercrime

Continued from last page

Alternate Forms of Cybercrime										
Cyber Crime Case	**Attacker Characteristics**	**Date of Incident**	**Jurisdictional Origin**	**Jurisditional Target**	**Target(s) of attack**	**Methodology of Attack**	**Indictment(s)**	**Responding Entity**	**Case information** (legal provision that case was charged under)	**Resources**
National Association of Software and Service Companies vs Ajay Sood & others	A placement company involved in headhunting and recruitment.	Mar-05	India	India	Software and Service Companies	Phishing		Delhi HC issued judgement in the lawsuit	"The Delhi HC stated that even though there is no specific legislation in India to penalize phishing, it held phishing to be an illegal act by defining it under Indian law as "a misrepresentation made in the course of trade leading to confusion as to the source and origin of the e-mail causing immense harm not only to the consumer but even to the person whose name, identity or password is misused." The court held the act of phishing as passing off and tarnishing the plaintiff's image. The defendants were operating a placement agency involved in head-hunting and recruitment. In order to obtain personal data, which they could use for purposes of headhunting, the defendants composed and sent e-mails to third parties in the name of Nasscom. The high court recognised the trademark rights of the plaintiff and passed an ex-parte adinterim injunction restraining the defendants from using the trade name or any other name deceptively similar to Nasscom. The court further restrained the defendants from holding themselves out as being associates or a part of Nasscom."	

A
APPENDIX
TABLE A

Alternate Forms of Cybercrime

Continued from last page

Alternate Forms of Cybercrime										
Cyber Crime Case	**Attacker Characteristics**	**Date of Incident**	**Jurisdictional Origin**	**Jurisditional Target**	**Target(s) of attack**	**Methodology of Attack**	**Indictment(s)**	**Responding Entity**	**Case information** (legal provision that case was charged under)	**Resources**
SMC Pneumatics India Pvt. Ltd. v. Jogesh Kwatra	Employee at company bringing lawsuit.	2001	India	India	SMC Pnuematics India Pvt. Ltd.	Harassment		Court of Delhi	"After hearing detailed arguments of Counsel for Plaintiff, Hon'ble Judge of the Delhi High Court passed an ex-parte ad interim injunction observing that a prima facie case had been made out by the plaintiff. Consequently, the Delhi High Court restrained the defendant from sending derogatory, defamatory, obscene, vulgar, humiliating and abusive emails either to the plaintiffs or to its sister subsidiaries all over the world including their Managing Directors and their Sales and Marketing departments. Further, Hon'ble Judge also restrained the defendant from publishing, transmitting or causing to be published any information in the actual world as also in cyberspace which is derogatory or defamatory or abusive of the plaintiffs."	

A
APPENDIX

TABLE A

Alternate Forms of Cybercrime

Continued from last page

Alternate Forms of Cybercrime										
Cyber Crime Case	**Attacker Characteristics**	**Date of Incident**	**Jurisdictional Origin**	**Jurisditional Target**	**Target(s) of attack**	**Methodology of Attack**	**Indictment(s)**	**Responding Entity**	**Case information** (legal provision that case was charged under)	**Resources**
Vyakti Vikas Kendra, India Public Charitable Trust THR Trustee Mahesh Gupta & ORS vs. Jitender Baggaa & ANR.	Defendants posted defamtory material on blogger webpage	2013	India	India	4 individuals connected to the India Public Trust, His Holiness Sri Sri Ravi Shankar, and Art of Living Teacher.	Defendants posted a high volume of highly defamatory materials on an internet website and indiscriminantly sent defamatory emails. The materials included personal attacks or alleged defamation, parody or satire of individuals, distasteful imagery or language, and political or social commentary.			Defendant No.2 (D2) is an "intermediary" within the definition of Section 2(1)(w) and Section 79 of the Information Technology Act, 2000. Under Section 79(3)(b) of the IT Act, 2000, D2 is under an obligation to remove unlawful content if it receives actual notice from the affected party of any illegal content being circulated/published through its service. D2 is also bound to comply with Information Technology (Intermediaries Guidelines) Rules 2011. Rule 3(3) of the said rules read with Rule 3(2) requires an intermediary to observe due diligence or publish any information that is grossly harmful, defamatory, libellious, disparaging or otherwise unlawful. Rule 3(4) of the said rule provides obligation of an intermediary to remove such defamatory content within 36 hours from receipt of actual knowledge. The said rule is cited below for easy reference.	

A
APPENDIX
TABLE A

Miscellaneous Attacks (to demonstrate capability)

Miscellaneous Attacks (to demonstrate capability)										
Cyber Crime Case	**Attacker Characteristics**	**Date of Incident**	**Jurisdictional Origin**	**Jurisdicitonal Target**	**Target(s) of attack**	**What was stolen?**	**Methodology of Attack**	**Indict-ment(s)**	**Responding Entity**	**Resources**
Flame and Stuxnet	Allegedly Governments		U.S. & Israel	Iran, Lebanon, Syria, Sudan and Israeli occupied territories.	Intelligence and destroys capacity	N/A	Malware-spreads through bluetooth, controls, copies and destroys. Shows the power of cyber attacks.			http://rt.com/news/flame-stuxnet-kaspersky-iran-607 http://www.wired.com/2012/05/flame/
Operation Ghost Click		2007- Oct. 2011	Estonia	U.S.			Domain Name System (DNS) hacked millions of computers to make money from marketing companies through the manipulation of viewer data.			http://www.fbi.gov/news/stories/2011/november/malware_110911
Morpho Cyber Espionage	Corporate espionage group dubbed 'Morpho'	2012-present		US, Europe and Canada	High profile technology, internet, commodities, and pharmaceutical companies.	confidential information and intellectual property	Application of malware Mac OS X backdoor program known as OSX.Pintsized as well as windows backdoor program Backdoor. Jiripbot		Detection by individual companies and private sector entities such as Semantec.	http://www.computerweekly.com/news/4500249597/Symantec-uncovers-Morpho-cyber-espionage-operation

Miscellaneous Attacks (to demonstrate capability)

Continued from last page

Miscellaneous Attacks (to demonstrate capability)										
Cyber Crime Case	**Attacker Characteristics**	**Date of Incident**	**Jurisdictional Origin**	**Jurisdicitonal Target**	**Target(s) of attack**	**What was stolen?**	**Methodology of Attack**	**Indict-ment(s)**	**Responding Entity**	**Resources**
Pawn Storm	cyber espionage group	2014		U.S., Europe, and Pakistan	Military, diplomatic and defence industry	Data	Operation was dubbed 'pawn storm' because the attackers used two or more connected tools or tactics to attack a target. Used phishing and spear-phishing.Used javascript trick to target Microsoft Outlook Web Access then specifically crafted emails to manipulate targets into visiting bogus Micorsoft outlook web access pages where they would enter their credentials.		Researchers at Trend Micro uncovered the scheme.	http://www.computerweekly.com/news/2240233415/Researchers-uncover-sophisticated-cyber-espionage-campaign

B
APPENDIX
TABLE B1

Overview of Multilateral Instruments on Cybercrime

Explanatory Note: This Appendix is divided into two parts. The first part (Table B1) lists the major multilateral instruments on cybercrime and describes the binding nature of each instrument. The second part (Table B2) identifies by article in each instrument (listed across the top of the page) where the substantive cybercrime provision (listed in the left column) can be found in that instrument.

Multilateral Instrument	Binding Multilateral Instruments on Cybercrime	Non-binding Multilateral Instruments on Cybercrime
Instruments developed in the context of, or inspired by, CoE or EU	■ CoE, Convention on Cybercrime (2001), Additional Protocol to the Convention on Cybercrime (2003), and Convention on Protection of Children against Sexual Exploitation and Sexual Abuse (2007) ■ EU legislation including on e-Commerce (2000/31/EC), on Combating Fraud and Counterfeiting of Non-Cash Means of Payment (2001/413/JHA), on Personal Data (2002/58/EC as amended), on Attacks against Information Systems (2013/40/EU replacing 2005/222/JHA) and Proposal for 2005/222/JHA [COM(2010) 517 final], and on Child Pornography (2011/92/EU)	■ Commonwealth Model Laws on Computer and Computer-related Crime (2002) and Electronic Evidence (2002)
Instruments developed by CIS	■ CIS, Agreement on Cooperation among the States members of the CIS in Combating Offences related to Computer Information (2001)	
Instruments developed by SCO	■ SCO, Agreement between the Governments of the Member States of the SCO on Cooperation in the Field of International Information Security (2009)	
Instruments developed in the African context	■ ECOWAS, Directive on Fighting Cybercrime within ECOWAS (2011) ■ AU, African Union Convention on Cyber Security and Personal Data Protection (2014)	■ East African Community (EAC) Legal Framework for Cyberlaws (Draft) (2008) ■ Common Market for Eastern and Southern Africa (COMESA), Cyber Crime Model Bill (2011) ■ ITU, Harmonization of ICT Policies in Sub-Saharan Africa ("HIPSSA"), Southern African Development Community (SADC) Model Law on Computer Crime and Cybercrime (2013)
Instruments developed by Arab League	■ League of Arab States, Arab Convention on Combating Information Technology Offences (2010)	■ League of Arab States, Model Law on Combating Information Technology Offences (2004)
Instruments developed in the context of Pacific Islands		■ ITU, Information and Communications Capacity Building for Pacific Island Countries ("ICB4PAC"), Electronic Crimes : Knowledge-Based Report (Skeleton) (2013)
Instruments developed in the Caribbean context		■ ITU, Harmonization of ICT Policies, Legislation and Regulatory Procedures in the Caribbean (HIPCAR), Model Legislative Texts on Cybercrime/e-Crime (2012) and Electronic Evidence (2013) ■ Organization for Eastern Caribbean States (OECS), Electronic Crimes Bill (Fourth Draft) (2011) and Electronic Evidence Bill (Third Draft) (2011)

View citations at the end of this section page 403

B
APPENDIX
TABLE B2

Comparative Analysis of Provisions of Multilateral Instruments on Cybercrime

Definitions												
Definitions	**AU[1]**	**CIS[2]**	**CoE[3]**	**LAS[4]**	**SCO[5]**	**ECOWAS[6]**	**COMESA[9]**	**OECS[15]**	**The Commonwealth[10]**	**ITU, HIPCAR[11]**	**ITU, HIPSSA[12]**	**ITU, ICB4PAC[13]**
Computer/Information/ Electronic System	Art.1		Art. 1(a)	Art. 2(5)		Art. 1	Sec.1	Sec. 2	Sec. 3	Sec. 3(5)	Sec.3(5)	Sec. 3(13)
Computer (Electronic) data [Computer information, Data]	Art.1	Art. 1(b)	Art. 1(b)	Arts. 2(1), 2(3)		Art. 1	Sec. 1	Sec. 2	Sec. 3	Sec. 3(6)	Sec. 3(6)	Secs. 3(9), 3(18)
Subscriber information			Art. 18(3)	Art. 2(9)			Sec. 1	Sec. 2				
Traffic data			Art. 1(d)				Sec. 1	Sec. 2	Sec. 3	Sec. 3(18)	Sec. 3(22)	Sec. 3(24)
Service provider/ISP			Art. 1(c)	Art. 2(2)			Sec. 1	Sec. 2	Sec. 3	Sec. 3(17)	Sec. 3(21)	Sec. 3(20)

View citations at the end of this section page 403

B
APPENDIX
TABLE B2

Comparative Analysis of Provisions of Multilateral Instruments on Cybercrime

Substantive Law, Cybercrime Acts, Acts Directed against the Confidentiality, Integrity and Availability of Computer systems or Data, Criminalization												
Criminalization	**AU[1]**	**CIS[2]**	**CoE[3]**	**LAS[4]**	**SCO[5]**	**ECOWAS[6]**	**COMESA[9]**	**OECS[15]**	**The Commonwealth[10]**	**ITU, HIPCAR[11]**	**ITU, HIPSSA[12]**	**ITU, ICB4PAC[13]**
Illegal access to a computer system	Arts. 29(1)(a), 29(1)(b)		Art. 2	Art. 6(1)		Art. 4	Sec. 18	Secs. 4(1)(a), 4(2)	Sec. 5	Sec. 4	Sec. 4	Sec. 2
Illegal interception	Art. 29(2)(a)		Art. 3	Art. 7		Art. 8	Sec. 21		Sec. 8	Sec. 6	Sec. 6	Sec. 4
Illegal interference with computer data	Arts. 29(1)(e), 29(1)(f)	Art. 3 (1)(c)	Art.4.	Art. 8		Arts. 7, 9	Sec. 20(2)	Secs. 4(1)(d4)(1)(i), 4(2)	Sec. 6	Sec. 7	Sec. 7	Sec. 5
Illegal interference with a computer system	Art. 29(1)(d)	Art. 3 (1)(c)	Art. 5	Art. 6(2)(a)		Art. 6	Sec. 20(1)	Secs. 4(1)(d4)(1)(i), 4(2)	Sec. 6	Sec. 7	Sec. 7	Sec. 5
Misuse of devices	Art. 29(1)(h)	Art. 3(1)(b)	Art. 6	Art. 9		Art. 14	Sec. 22	Sec. 19	Sec. 9	Sec. 10	Sec. 10	Sec. 8
Illegal access to computer data		Art. 3(1)(a)	Art. 2				Sec. 19					
Illegal acquisition of computer data			Art. 2					Sec. 4(1)(b)		Sec. 8	Sec. 8	Sec. 6
Illegal remaining in a computer system	Art. 29(1)(c)					Art. 5				Sec. 5	Sec. 5	Sec. 3

View citations at the end of this section page 403

B
APPENDIX
TABLE B2

Comparative Analysis of Provisions of Multilateral Instruments on Cybercrime

Substantive Law, Cybercrime Acts, Acts Committed by Use of Computer Systems or Data, Computer-related Acts, Criminalization												
Criminalization	**AU[1]**	**CIS[2]**	**CoE[3, 8]**	**LAS[4]**	**SCO[5]**	**ECOWAS[6]**	**COMESA[9]**	**OECS[15]**	**The Commonwealth[10]**	**ITU, HIPCAR[11]**	**ITU, HIPSSA[12]**	**ITU, ICB4PAC[13]**
Computer-related forgery	Art. 29(2)(b)		Art. 7	Art. 10		Art. 10	Sec. 23	Sec.8		Sec. 11	Sec. 11	
Computer-related fraud	Art. 29(2)(d)		Art. 8	Art. 11		Art. 11	Sec. 24	Sec. 9		Sec. 12	Sec. 12	Sec. 10
Computer-related copyright and trademark offences		Art. 3(1)(d)	Art. 10	Art. 17								
Sending SPAM, etc.			Arts. 2 to 6, 8, 10 to 11				Sec. 19(7)	Sec. 5		Sec. 15	Sec. 19	Sec. 14
Computer-related identity offences			Arts. 2 to 6					Sec.6		Sec. 14	Sec. 15	Sec. 13
Computer-related solicitation of a child (grooming)			Lanzarote Conventi on, Art. 23									Sec. 19
Cyber-harassment										Sec. 18	Sec. 22	
Cyberstalking								Sec. 17				Sec. 17
Sending offensive messages through communication services								Sec. 5				

View citations at the end of this section page 403

B
APPENDIX
TABLE B2

Comparative Analysis of Provisions of Multilateral Instruments on Cybercrime

Substantive Law, Cybercrime Acts, Acts Committed by Use of Computer Systems or Data, Computer Content-related Acts, Criminalization												
Criminalization	**AU[1]**	**CIS[2]**	**CoE[3, 7]**	**LAS[4]**	**SCO[5]**	**ECOWAS[6]**	**COMESA[9]**	**OECS[15]**	**The Commonwealth[10]**	**ITU, HIPCAR[11]**	**ITU, HIPSSA[12]**	**ITU, ICB4PAC[13]**
Computer-related child pornography offence	Arts. 29(3)(1)(a) to 29(3)(1)(c)		Art 9.	Arts. 12(2), 12(3)		Arts. 16 to 18		Sec. 13	Sec. 10	Sec. 13	Sec. 13	Sec. 11
Computer-related dissemination of racist and xenophobic material	Art. 29(3)(1)(e)		Additional Protocol, Art. 3			Art. 20					Sec. 16(c)	
Computer-related racist and xenophobic motivated threat	Art. 29(3)(1)(f)		Additional Protocol, Art. 4			Art. 21						
Computer-related racist and xenophobic motivated insult	Art. 29(3)(1)(g)		Additional Protocol, Art. 5			Art. 22					Sec. 17	
Computer-related denial or justification of genocide or crimes against humanity	Art. 29(3)(1)(h)		Additional protocol, Art. 6			Art. 23					Sec. 18	
Computer-related acts in support of terrorism			Arts 2 to 8, 11 to 12	Arts. 15(1) to 15(3)								
Cyber-defamation								Sec. 7				Sec. 20
Computer-related pornography offence				Arts. 12(1), 13		Arts. 16 to 18						Sec. 12
Facilitation of access of a child to pornography	Art. 29(3)(1)(d)		Art. 9			Art. 19					Sec. 14	
Computer-related religious offences				Art. 15(4)								Sec. 21

View citations at the end of this section page 403

Comparative Analysis of Provisions of Multilateral Instruments on Cybercrime

Substantive Law, Other Cybercrime Acts, Criminalization												
Criminalization	**AU[1]**	**CIS[2]**	**CoE[3]**	**LAS[4]**	**SCO[5]**	**ECOWAS[6]**	**COMESA[9]**	**OECS[15]**	**The Commonwealth[10]**	**ITU, HIPCAR[11]**	**ITU, HIPSSA[12]**	**ITU, ICB4PAC[13]**
Computer-related money laundering offence				Art. 16(1)								
Computer-related illicit trafficking				Arts. 16(2) to 16(4)								
Illegal online gambling				Art. 13								Sec. 18
Computer-related extortion							Sec. 25					
Computer-related acts involving personal information/personal data	Art. 29(2)(e)		Arts 2 & 4			Art. 12						
Computer-related breach of secrecy	Art. 31(2)(c)		Arts 2 & 3									
Use of forged/fraudulently obtained data	Art. 29(2)(c)		Arts 7 & 8		Art. 13							
Illicit use of electronic payment tools				Art. 18								
Computer-related acts against privacy			Arts 2 & 4	Art. 14				Sec.11				
Disclosure of details of an investigation by a service provider			Arts 16, 20 & 21					Sec. 29(2)	Sec. 21(1)	Sec. 16	Sec. 20	Sec. 15
Failure to provide assistance in an investigation			Arts 16, 18, 20 & 21						Sec. 13(2)	Sec. 17	Sec. 21	Sec. 16
Failure to comply with in an investigative request			Arts 16, 18, 20 & 21					Secs. 23(4)(b),23(5)				
Obstruction of an investigation								Secs. 23(4)(a), 23(5)				

View citations at the end of this section page 403

B
APPENDIX
TABLE B2

Comparative Analysis of Provisions of Multilateral Instruments on Cybercrime

Substantive Law, Sanctions and Liabilities												
Substantive Law, Sanctions and Liabilities	**AU[1]**	**CIS[2]**	**CoE[3]**	**LAS[4]**	**SCO[5]**	**ECOWAS[6]**	**COMESA[9]**	**OECS[15]**	**The Commonwealth[10]**	**ITU, HIPCAR[11]**	**ITU, HIPSSA[12]**	**ITU, ICB4PAC[13]**
Aggravating circumstance for conventional offence committed by means of a computer system	Art. 30(1)(b)			Art. 21		Art. 24						
Attempt and aiding or abetting	Arts. 29(1)(a-f), 29(2)(a)		Art. 11	Art 19.			Sec. 26					Sec. 22
Corporate liability	Art. 30(2)		Art. 12	Art. 20		Art. 27	Sec. 27					Sec. 22
Sanctions and measures	Art. 31		Art. 13			Arts. 28, 29						

View citations at the end of this section page 403

B
APPENDIX
TABLE B2

Comparative Analysis of Provisions of Multilateral Instruments on Cybercrime

Procedural Law												
Procedural Law	**AU[1]**	**CIS[2]**	**CoE[3]**	**LAS[4]**	**SCO[5]**	**ECOWAS[6]**	**COMESA[9]**	**OECS[15]**	**The Commonwealth[10]**	**ITU, HIPCAR[11]**	**ITU, HIPSSA[12]**	**ITU, ICB4PAC[13]**
Scope of procedural provisions			Art. 14	Art. 22			Sec. 28					
Procedural conditions and safeguards			Art. 15				Sec. 32					
Expedited preservation of stored computer data	Art. 31(3)(d)		Art. 16	Art. 23		Art. 31	Sec. 33	Sec. 20	Sec. 17	Sec. 23	Sec. 28	Sec. 28
Expedited preservation and partial disclosure of traffic data			Art. 17	Art. 24			Sec. 34	Sec. 21	Sec. 18	Sec. 24	Sec. 29	Sec. 29
Expedited preservation of computers or storage media							Sec. 35					
Production order			Art. 18	Art. 25			Sec. 36	Sec. 22	Sec. 15	Sec .22	Sec. 27	Sec. 27
Search and Seizure of a computer system or data	Arts. 31(3) (a), 31(3)(b)		Arts. 19(1) to 19(3)	Arts. 26, 27(1)		Art. 30	Secs. 37(1) to 37(3)		Secs. 12, 14	Sec. 20	Sec. 25	Sec. 25
Real-time collection of traffic data			Art. 20	Art. 28			Sec. 38	Sec. 24	Sec. 19	Sec. 25	Sec. 30	Sec. 30
Interception of content data	Art. 31 (3)(e)		Art. 21	Art. 29			Sec. 39		Sec. 18	Sec. 26	Sec. 31	Sec. 31
Use of remote forensic tools										Sec. 27	Sec. 32	Sec. 32
Trans-border access to stored computer data			Art. 32	Art. 40			Sec. 49					
Provision of assistance in investigation	Art. 31(3)(e)		Art. 19(4)	Art. 27(2)			Sec, 37(4)		Sec. 13	Sec. 21	Sec. 26	Sec. 26
Retention of computer Data							Secs. 29 to 31					

View citations at the end of this section page 403

B
APPENDIX
TABLE B2

Comparative Analysis of Provisions of Multilateral Instruments on Cybercrime

Admissibility of Electronic Evidence												
Admissibility of electronic evidence	**AU[1]**	**CIS[2]**	**CoE[3]**	**LAS[4]**	**SCO[5]**	**ECOWAS[6]**	**COMESA[9]**	**OECS[15]**	**The Commonwealth[10]**	**ITU, HIPCAR[11]**	**ITU, HIPSSA[12]**	**ITU, ICB4PAC[13]**
Admissibility of electronic evidence	Arts. 6(6), 29(4)					Art. 32	Sec. 5(1)		Sec. 20	Sec. 5	Sec. 24	Sec. 24
Admissibility of foreign electronic evidence										Sec. 16		

View citations at the end of this section page 403

B
APPENDIX
TABLE B2

Comparative Analysis of Provisions of Multilateral Instruments on Cybercrime

Jurisdiction												
Jurisdiction	**AU[1]**	**CIS[2]**	**CoE[3]**	**LAS[4]**	**SCO[5]**	**ECOWAS[6]**	**COMESA[9]**	**OECS[15]**	**The Commonwealth[10]**	**ITU, HIPCAR[11]**	**ITU, HIPSSA[12]**	**ITU, ICB4PAC[13]**
Committed within the territory			Art. 22(1)(a)	Art. 30(1)(a)			Sec. 40(1)(a)	Sec. 3 (a)	Sec. 4(a)	Sec. 19(a)	Sec. 23(a)	Sec. 23(a)
Committed on a registered ship or aircraft			Arts. 22(1)(b), 22(1)(c)	Arts. 30(1)(b), 30(1)(c)			Sec. 40(2)		Sec. 4(b)	Sec. 19(b)	Sec. 23(b)	
Using a computer system/data within the territory							Sec. 40(1)(b)					
Directed against a computer system/data within the territory							Sec. 40(1)(c)					
Nationality principle (Offender)			Art. 22(1)(d)	Art. 30(1)(d)			Secs. 40(3)(a), 40(3)(b)		Secs. 4(c), 4(d)	Sec. 19(c)	Secs. 23(c), 23(d)	Secs. 23(b), 23(c)
State interest principles				Art. 30(1)(e)								
Jurisdiction when extradition refused			Art. 22(3)	Art. 30(2)			Sec. 40(4)					
Concurrent jurisdiction			Art. 22(4)	Art. 30(3)			Sec. 40(5)					
Establishment of place of offence							Sec. 40(6)					
Dual criminality			Art. 22(1)(d)	Art. 30(1)(d)			Sec. 40(3)(a)		Sec. 4(d)	Sec. 19(c)	Sec. 23(d)	Sec. 23(b)
Reservation			Art. 22(2)				Sec. 40(7)					

View citations at the end of this section page 403

Comparative Analysis of Provisions of Multilateral Instruments on Cybercrime

International Cooperation, International Cooperation: General Principles												
International Cooperation: General Principles	**AU[1]**	**CIS[2]**	**CoE[3]**	**LAS[4]**	**SCO[5]**	**ECOWAS[6]**	**COMESA[9]**	**OECS[15]**	**The Commonwealth[10]**	**ITU, HIPCAR[11]**	**ITU, HIPSSA[12]**	**ITU, ICB4PAC[13]**
International cooperation: general principles	Art. 28	Art. 5	Art. 23		Arts. 3 to 5	Art. 33	Sec. 41					

International Cooperation, Extradition: General Principles												
Extradition: General Principles	**AU[1]**	**CIS[2]**	**CoE[3]**	**LAS[4]**	**SCO[5]**	**ECOWAS[6]**	**COMESA[9]**	**OECS[15]**	**The Commonwealth[10]**	**ITU, HIPCAR[11]**	**ITU, HIPSSA[12]**	**ITU, ICB4PAC[13]**
Extradition: general principles			Art. 24	Art. 31			Sec. 42					
Dual criminality			Art. 24(1)(a)	Art. 31(1)(a)			Sec. 42(1)					
Extraditable Offences			Arts. 24(1), 24(2), 24(4)	Arts. 31(1), 31(2), 31(4)			Secs. 42(1), 42(3)	Sec. 31				

View citations at the end of this section page 403

B
APPENDIX
TABLE B2

Comparative Analysis of Provisions of Multilateral Instruments on Cybercrime

International Cooperation, Mutual Assistance (MA): General Principles [Mutual Legal Assistance (MLA): General Rules]												
MA: General principles (MLA: General Rules)	**AU[1]**	**CIS[2]**	**CoE[3]**	**LAS[4]**	**SCO[5]**	**ECOWAS[6]**	**COMESA[9]**	**OECS[15]**	**The Commonwealth[10]**	**ITU, HIPCAR[11]**	**ITU, HIPSSA[12]**	**ITU, ICB4PAC[13]**
MA: General principles (MLA–General Rules)	Art. 28 (2)	Art. 6	Arts. 25-27	Arts. 32 to 34			Secs. 43 to 45					
Expedited means of communication or other urgent channels		Art. 6(2)	Arts. 25(3), 27(9)	Arts. 32(3), 34(8)			Secs. 43(2), 45(8)					
Dual criminality	Art. 28(2)		Art. 25(5)	Art. 32(5)			Sec. 43(4)					
Spontaneous (Unsolicited) information		Art. 6(1)	Art. 26	Art. 33			Sec. 44					
Refusal of cooperation/ assistance		Art. 8	Arts. 25(4), 27(4)	Art. 35			Secs. 43(3), 45(5)					
Confidentiality of information to be provided and Limitation on Use		Art. 9	Art. 28	Art. 36	Art. 6		Secs. 45(9), 45(10)					
Confidentiality of the fact of any request made and its subject			Art. 27(8)	Art. 34(7)			Sec. 45(7)					

View citations at the end of this section page 403

B
APPENDIX
TABLE B2

Comparative Analysis of Provisions of Multilateral Instruments on Cybercrime

International Cooperation, Mutual Assistance (MA): Specific Provisions [Mutual Legal Assistance (MLA): Specific Rules]												
MA: Specific Provisions (MLA: Specific Rules)	**AU[1]**	**CIS[2]**	**CoE[3]**	**LAS[4]**	**SCO[5]**	**ECOWAS[6]**	**COMESA[9]**	**OECS[15]**	**The Commonwealth[10]**	**ITU, HIPCAR[11]**	**ITU, HIPSSA[12]**	**ITU, ICB4PAC[13]**
Expedited preservation of stored computer data			Art. 29	Art. 37			Sec. 46					
Expedited disclosure of preserved traffic data			Art. 30	Art. 38			Sec. 47					
MA: Accessing of stored computer data			Art. 31	Art. 39			Sec. 48					
Trans-border access to stored computer data			Art. 32	Art. 40			Sec. 49					
MA: Real-time collection of traffic data			Art. 33	Art. 41			Sec. 50					
MA: Interception of content data			Art. 34	Art. 42			Sec. 51					

View citations at the end of this section page 403

B
APPENDIX
TABLE B2

Comparative Analysis of Provisions of Multilateral Instruments on Cybercrime

International Cooperation, 24-7 Network												
24-7 Network	**AU[1]**	**CIS[2]**	**CoE[3]**	**LAS[4]**	**SCO[5]**	**ECOWAS[6]**	**COMESA[9]**	**OECS[15]**	**The Commonwealth[10]**	**ITU, HIPCAR[11]**	**ITU, HIPSSA[12]**	**ITU, ICB4PAC[13]**
24/7 Network			Art. 35	Art. 43			Sec. 52					

View citations at the end of this section page 403

Comparative Analysis of Provisions of Multilateral Instruments on Cybercrime

Service Provider Liability and Responsibility												
Service Provider Liability and Responsibility	**AU[1]**	**CIS[2]**	**CoE[3]**	**LAS[4]**	**SCO[5]**	**ECOWAS[6]**	**COMESA[9]**	**OECS[15]**	**The Commonwealth[10]**	**ITU, HIPCAR[11]**	**ITU, HIPSSA[12]**	**ITU, ICB4PAC[13]**
No general monitoring obligation							Sec. 17(1)			Sec. 28	Sec. 33	Sec. 33
Voluntary Supply (Provision) of Information							Sec. 17(2)					
Take-down notifications							Sec. 16					
Liability of access providers							Sec. 12			Sec. 29	Sec. 34	Sec. 34
Liability of caching providers							Sec. 13			Sec. 31	Sec. 35	Sec. 36
Liability of hosting providers							Sec. 14			Sec. 30	Sec. 36	Sec. 35
Liability of hyperlink providers							Sec. 15			Sec. 32	Sec. 37	Sec 37
Liability of search engine providers										Sec. 33	Sec. 38	Sec. 38

View citations at the end of this section page 403

C
APPENDIX
TABLE C

National Legal Frameworks on Combating Cybercrime (Assessment Table)

Explanatory Note: This Table reviews the legal frameworks of 196 countries, based on initial research of publicly available laws, regulations and electronic data which were verified and updated based on a review of ITU[1] and UNCTAD data,[1] as well as UNCTAD's Cyber Law Tracker[1]. This Table provides an overview of national legal frameworks using the working definition of cybercrime adopted in section 2 A, with particular reference to whether acts against the confidentiality, integrity and availability of computer systems or data ("core" cybercrime acts) are criminalized. However, states are not deemed to have domestic legislation regarding cybercrime if "core" cybercrime acts are not criminalized.[1] No distinction is made between laws on the basis of naming: some states specifically refer to "cybercrime" or some other similar term, in their laws, while for other states use the same terms found in their penal or criminal code.

National Legal Frameworks on Combating Cybercrime[1]						
Country Name[2]	Has domestic legislation regarding cybercrime	Name of domestic legislation regarding cybercrime	International or Regional Instrument[3]			
			Budapest Convention	Arab Convention	CIS Agreement	SCO Agreement
Afghanistan	No		No	No	No	No
Albania	Yes	Criminal Code (last amended in 2013) (*e.g.*, Article 192/b)	{Has signed and/or ratified (or acceded to)}	No	No	No
Algeria	Yes	Law No. 09-04 of 14 Sha'ban 1430 Corresponding to 5 August 2009 Containing Specific Rules on the Prevention and Fight Against Information Technologies and Communication's Crimes (enacted in 2009)	No	{Has signed and/or ratified (or acceded to)}	No	No
Andorra	Yes	Penal Code [Article 225 (Computer Damage)]	{Has signed and/or ratified (or acceded to)}	No	No	No
Angola	No & Draft Law	▪ Draft Law to Combat Crime in the Field of ICT and Services for the Information Society (2011) ▪ Preliminary Draft Penal Code [*e.g.*, Article 399 (Computer Damage)]	No	No	No	No
Antigua and Barbuda	Yes	Electronic Crimes Act, 2013	No	No	No	No
Argentina	Yes	Penal Code (enacted by Law No. 11, 179 of 1984 and amended by Law No. 26,388 of 2008) (*e.g.*, Sections 153B, 153C, and 153D)	Invited to accede	No	No	No
Armenia	Yes	Criminal Code (adopted on 18 April 2003), Chapter 24. Crimes against computer information security (Articles 251-257)	{Has signed and/or ratified (or acceded to)}	No	{Has signed and/or ratified (or acceded to)}	No

View citations at the end of this section page 404

C
APPENDIX
TABLE C

National Legal Frameworks on Combating Cybercrime (Assessment Table)

National Legal Frameworks on Combating Cybercrime[1]						
Country Name[2]	Has domestic legislation regarding cybercrime	Name of domestic legislation regarding cybercrime	International or Regional Instrument[3]			
			Budapest Convention	Arab Convention	CIS Agreement	SCO Agreement
Australia	Yes	Criminal Code [enacted by Act No. 12 of 1995 as amended up to Act No. 50 of 2010 and further amended by Act No. 120 of 2012 (Cybercrime Legislation Amendment Act 2012)], Chapter 10.National Infrastructure, Part 10.7 —Computer offences (Articles 476.1 to 478.4)	{Has signed and/or ratified (or acceded to)}	No	No	No
Austria	Yes	Criminal Code (Sections 118a, 119, 119a, 126a, 126b, 126c, 148a, 225a)	{Has signed and/or ratified (or acceded to)}	No	No	No
Azerbaijan	Yes	▪ Criminal Code (adopted on 30 September 1999 and came into force on 1 September 2000), Chapter 30. Crimes in Sphere of the Computer Information (Articles 271, 272, and 273) ▪ Criminal Procedure Code (adopted on 14 July 2000)	{Has signed and/or ratified (or acceded to)}	No	{Has signed and/or ratified (or acceded to)}	No
Bahamas, The	Yes	Computer Misuse Act, 2006	No	No	No	No
Bahrain	Yes	Law No. 60 of 2014 concerning Information Technology Crimes	No	{Has signed and/or ratified (or acceded to)}	No	No
Bangladesh	Yes	Information & Communication Technology Act, 2006 [amended by Information & Communication Technology (Amendment) Act, 2013], Chapter VII. Offenses, Investigation, Adjudication, Penalties etc. (Sections 54 to 90)	No	No	No	No
Barbados	Yes	Computer Misuse Act, 2005	No	No	No	No
Belarus	Yes	Criminal Code (Penal Code) (enacted in 1999) (as amended up to 2013)], Section XII. Chapter 31. Crimes against information security (Articles 349-355)	No	No	{Has signed and/or ratified (or acceded to)}	No
Belgium	Yes	▪ Criminal Code (amended by Law on computer crime of 28 November 2000) (Article 210bis; Article 504quater, Article 550bis, Article 550ter) ▪ Criminal Procedure Code (Article 39bis; Article 88ter; Article 88quater; Article 90quater)	{Has signed and/or ratified (or acceded to)}	No	No	No

View citations at the end of this section page 404

C
APPENDIX
TABLE C

National Legal Frameworks on Combating Cybercrime (Assessment Table)

National Legal Frameworks on Combating Cybercrime[1]						
Country Name[2]	Has domestic legislation regarding cybercrime	Name of domestic legislation regarding cybercrime	International or Regional Instrument[3]			
			Budapest Convention	Arab Convention	CIS Agreement	SCO Agreement
Belize	No		No	No	No	No
Benin	No & Draft Law	▪ Draft Decree No. 200/MISP/DC/SGM/DGPN/SERCT/DER/SA related to the creation of a division in charge of the fight against internet crime ▪ Draft Law on the Fight against Cybercrime	No	No	No	No
Bhutan	Yes	Information, Communications and Media Act 2006, Provisions relating to certain cyber offenses (Sections 171 to 182)	No	No	No	No
Bolivia	Yes	▪ Penal Code (Articles 363bis and 363 ter)	No	No	No	No
Bosnia and Herzegovina	Yes	Criminal Code (2003, amended in 2013) (Chapter 24A. Criminal Offences against Computer Data Security) (Articles 292a to 292e)	{Has signed and/or ratified (or acceded to)}	No	No	No
Botswana	Yes	Cybercrime and Computer Related Crimes (Chapter 08: 06) (Date of commencement: 28 Dec. 2007)	No	No	No	No
Brazil	Yes	Criminal Code (enacted by Law No. 2, 848 of 1940, and amended by Law No. 9,983 of 2000, Law No. 11, 829 of 2008, Law No. 12, 735 of 2012, and Law No. 12, 737 of 2012) [*e.g.*, Article 154 – A (Trespass of a computing device)]	No	No	No	No
Brunei Darussalam	Yes	▪ Computer Misuse Act, 2007 (Chapter 194) ▪ Penal Code [enacted in 1951, as last amended by Penal Code (Amendment) Order, 2012]	No	No	No	No
Bulgaria	Yes	▪ Penal Code, Chapter 9, Computer Crimes (Articles 319a to Articles 319f) ▪ Criminal Procedure Code	{Has signed and/or ratified (or acceded to)}	No	No	No
Burkina Faso	Yes & Draft Law	▪ Penal Code, 1996 [Chapter V. Offences Concerning Computers (Articles 541-548)] ▪ Draft Law on Cybercrime	No	No	No	No

View citations at the end of this section page 404

C
APPENDIX
TABLE C

National Legal Frameworks on Combating Cybercrime (Assessment Table)

National Legal Frameworks on Combating Cybercrime[1]						
Country Name[2]	Has domestic legislation regarding cybercrime	Name of domestic legislation regarding cybercrime	International or Regional Instrument[3]			
			Budapest Convention	Arab Convention	CIS Agreement	SCO Agreement
Burundi	Yes	Penal Code (enacted in 2009) (Articles 467-470)	No	No	No	No
Cabo Verde	Yes	Penal Code [Article 187 (Illegal Computer Processing)]	No	No	No	No
Cambodia	Yes & Draft Law	▪ Draft Cybercrime Law ▪ Criminal Code (Articles 317 to 320, Articles 427 to 432)	No	No	No	No
Cameroon	Yes	Law No. 12 of 2010 on Cybersecurity and Cybercrime (also known as "Law No. 12 of 2010 Relating to Cybersecurity and Cybercriminality")	No	No	No	No
Canada	Yes	Criminal Code [last amended by "Protecting Canadians from Online Crime Act" (assented on 9 December 2014)]	{Has signed and/or ratified (or acceded to)}	No	No	No
Central African Republic	No		No	No	No	No
Chad	Yes	Law No. 14 of 2014 regarding Electronic Communications (Articles 114, 115, 116, and 120)	No	No	No	No
Chile	Yes	Law on Automated Data Processing Crimes (also known as "Law No. 19,223 of 1993 on Categories of Computer-Related Offenses")	{Has signed and/or ratified (or acceded to)}	No	No	No
China	Yes	Criminal Law (adopted in 1979 and last amended in 2011) (Articles 285, 286 and 287)	No	No	No	{Has signed and/or ratified (or acceded to)}
Colombia	Yes	Penal Code [enacted by Law No. 599 of 2000, amended by Law No. 1273 of 2009 (Protection of Information and Data), and last amended by Law No. 1336 of 2009] (Article 269A to Article 269J)	Invited to accede	No	No	No
Comoros	No		No	No	No	No
Congo, Dem. Rep.	No		No	No	No	No

View citations at the end of this section page 404

C
APPENDIX
TABLE C

National Legal Frameworks on Combating Cybercrime (Assessment Table)

National Legal Frameworks on Combating Cybercrime[1]						
Country Name[2]	Has domestic legislation regarding cybercrime	Name of domestic legislation regarding cybercrime	International or Regional Instrument[3]			
			Budapest Convention	Arab Convention	CIS Agreement	SCO Agreement
Congo, Rep.	No & Draft Law	Draft Law on the Fight against Cybercrime (in progress)	No	No	No	No
Costa Rica	Yes	Penal Code [enacted by Law No. 4573 and amended by Law No. 9048 (10 July 2012) and last amended by Law No. 9135 (24 April 2013)] (Articles 196, 196bis, 217bis, 229bis)	Invited to accede	No	No	No
Cote d'Ivoire	Yes	Act No. 2013-451 dated 19 June 2013 on the fight against cybercrime	No	No	No	No
Croatia	Yes	■ Criminal Code (Enacted by Text No. 2498 of 2011, Amended by Text No. 3076 of 2012, Date of Entry into Force: 1 January 2013) (Articles 266 –272) ■ Criminal Procedure Code	{Has signed and/or ratified (or acceded to)}	No	No	No
Cuba[5]	No		No	No	No	No
Cyprus	Yes	Law Ratifying the Cybercrime Convention of 2001 (No. 22(III)/2004)	{Has signed and/or ratified (or acceded to)}	No	No	No
Czech Republic	Yes	Criminal Code, Act No. 40 of 2009 Coll. of January 8, 2009 (effective in 2010 and as amended in 2011) (Sections 230, 231, and 232)	{Has signed and/or ratified (or acceded to)}	No	No	No
Denmark	Yes	Penal Code (Sections 263-263a)	{Has signed and/or ratified (or acceded to)}	No	No	No
Djibouti	Yes	Penal Code [Chapter VII. Offences Concerning Computers (Articles 548-555)]	No	No	No	No
Dominica	No & Draft Law	■ Electronic Crime Bill ■ Computer and Computer Related Crimes Bill, 2005	No	No	No	No
Dominican Republic	Yes	Law No. 53 of 2007 on High Technology Crimes (adopted in 2007)	{Has signed and/or ratified (or acceded to)}	No	No	No

View citations at the end of this section page 404

C
APPENDIX
TABLE C

National Legal Frameworks on Combating Cybercrime (Assessment Table)

National Legal Frameworks on Combating Cybercrime[1]						
Country Name[2]	Has domestic legislation regarding cybercrime	Name of domestic legislation regarding cybercrime	International or Regional Instrument[3]			
			Budapest Convention	Arab Convention	CIS Agreement	SCO Agreement
Ecuador	Yes	Organic Comprehensive Criminal Code (Law No. 180 of 2014), (Articles 229 to 234)	No	No	No	No
Egypt, Arab Rep.	Yes & Draft Law	▪ Penal Code (Article 309bis) ▪ Telecommunication Regulation Law (Law No. 10 of 2003) (Article 78) ▪ Draft Cybercrime Law (2016)	No	{Has signed and/or ratified (or acceded to)}	No	No
El Salvador	Yes	Special Law against Computer and Related Crimes (Published on 26 Feb. 2016)	No	No	No	No
Equatorial Guinea	No		No	No	No	No
Eritrea	Yes	Penal Code (2015) [Art. 374 (Unauthorized Use of a Computer), Art. 375 (Aggravated Unauthorized Use of a Computer)]	No	No	No	No
Estonia	Yes	▪ Criminal Code (Penal Code) (as amended up to Act RT I, 29.12.2011, 1) (Sections 206 to 208) ▪ Criminal Procedure Code	{Has signed and/or ratified (or acceded to)}	No	No	No
Ethiopia	Yes & Draft Law	▪ Criminal Code (Proclamation No.414/2004), [Part II. Special Part; Book VI. Crimes against Property; Title I. Crimes against rights in property; Section II. Computer Crimes (Articles 706-711)] ▪ Draft Cybercrime Law (2016) [called "(Draft) Computer Crime Proclamation No…/2016"]	No	No	No	No
Fiji	Yes	Crimes Decree 2009 (Decree No. 44 of 2009) [Chapter III – Criminal Offenses, Part 17 — Fraudulent Conduct, Division 6 — Computer Offences, Articles 336-346]	No	No	No	No
Finland	Yes	▪ Criminal Code (Chapter 38 - Data and communications offences, Sections 1 to 12) ▪ Criminal Procedure Act	{Has signed and/or ratified (or acceded to)}	No	No	No

View citations at the end of this section page 404

C
APPENDIX
TABLE C

National Legal Frameworks on Combating Cybercrime (Assessment Table)

National Legal Frameworks on Combating Cybercrime[1]						
Country Name[2]	Has domestic legislation regarding cybercrime	Name of domestic legislation regarding cybercrime	International or Regional Instrument[3]			
			Budapest Convention	Arab Convention	CIS Agreement	SCO Agreement
France	Yes	▪ Criminal Code [Book III. Felonies and Misdemeanors against Property, Title II. Other offences against Property, Chapter III. Unauthorized Access to Automated Data Processing (Articles 323-1 to 323-7)] ▪ Criminal Procedure Code ▪ Law No.2004-575 of 21 June 2004 regarding Confidence in the Digital Economy	{Has signed and/or ratified (or acceded to)}	No	No	No
Gabon	No & Draft Law	Draft Law on Cybercrime (in progress)	No	No	No	No
Gambia	Yes	Information and Communications Act, 2009 (amended by "Information and Communication (Amendment) Act, 2013"), Chapter 3- Information Society Issues (Sections 163-173)	No	No	No	No
Georgia	Yes	Criminal Code, Chapter 35. Computer crimes (Articles 284, 285 and 286)	{Has signed and/or ratified (or acceded to)}	No	No	No
Germany	Yes	▪ German Criminal Code (*e.g.*, Section 202a, Section 303a, Section 303b) ▪ German Code of Criminal Procedure	{Has signed and/or ratified (or acceded to)}	No	No	No
Ghana	Yes	▪ Electronic Transactions Act (Act No. 772 of 2008), [Cyber inspectors (Sections 98 to 106), Cyber offences (Sections 107 to 140)] ▪ Criminal Code (Act 29 of 1960) (also known as "Criminal Offences Act")	No	No	No	No
Greece	Yes	Penal Code (amended by Law 1805/1988) (Articles 370, 370C, 386)	{Has signed and/or ratified (or acceded to)}	No	No	No
Grenada	Yes	▪ Electronic Crimes Act of 2013 ▪ [published in the Official Gazette on October 3, 2013 according to the International Press Institute (IPI)] ▪ Electronic Transactions Act, 2008 (Section 43)	No	No	No	No

View citations at the end of this section page 404

C
APPENDIX
TABLE C

National Legal Frameworks on Combating Cybercrime (Assessment Table)

National Legal Frameworks on Combating Cybercrime[1]						
Country Name[2]	Has domestic legislation regarding cybercrime	Name of domestic legislation regarding cybercrime	International or Regional Instrument[3]			
			Budapest Convention	Arab Convention	CIS Agreement	SCO Agreement
Guatemala	Yes	Penal Code (Articles 274A to 274G)	No	No	No	No
Guinea	No		No	No	No	No
Guinea-Bissau	No		No	No	No	No
Guyana	No		No	No	No	No
Haiti	No		No	No	No	No
Holy See	No data		No	No	No	No
Honduras	No		No	No	No	No
Hungary	Yes	Criminal Code (promulgated on 13 July 2012) (Sections 423-424)	{Has signed and/or ratified (or acceded to)}	No	No	No
Iceland	Yes	Penal Code (Articles 155, 157, 158, 228, 249a, and 257)	{Has signed and/or ratified (or acceded to)}	No	No	No
India	Yes	Information Technology Act, 2000 [amended by Information Technology (Amendment) Act, 2008] (Sections 43 to 45, Sections 65 to 78)	No	No	No	No
Indonesia	Yes	Law Concerning Electronic Information and Transactions (No. 11 of 2008) (Articles 27 to 37, Articles 45 to 52)	No	No	No	No
Iran, Islamic Rep.	Yes	Computer Crimes Law	No	No	No	No

View citations at the end of this section page 404

C
APPENDIX
TABLE C

National Legal Frameworks on Combating Cybercrime (Assessment Table)

National Legal Frameworks on Combating Cybercrime[1]						
Country Name[2]	Has domestic legislation regarding cybercrime	Name of domestic legislation regarding cybercrime	International or Regional Instrument[3]			
			Budapest Convention	Arab Convention	CIS Agreement	SCO Agreement
Iraq	No & Draft Law	Draft Informatics Crimes Law, 2010 (Revoked in 2013)	No	{Has signed and/or ratified (or acceded to)}	No	No
Ireland	Yes	▪ Criminal Justice (Theft and Fraud Offences) Act, 2001, Section 9 ▪ Criminal Damages Act, 1991	{Has signed and/or ratified (or acceded to)}	No	No	No
Israel	Yes	Computers Law of 1995 [Chapter 2. Computer Offences (Sections 2 to 6)]	{Has signed and/or ratified (or acceded to)}	No	No	No
Italy	Yes	Criminal Code (amended by Law No. 547 of 23 December 1993. Amendment of the Provisions of the Penal Code & the Code of Criminal Procedure in Relation to Computer Criminality)	{Has signed and/or ratified (or acceded to)}	No	No	No
Jamaica	Yes	Cybercrimes Act, 2010	No	No	No	No
Japan	Yes	Act on Prohibition of Unauthorized Computer Access (enacted in 1999 and amended in 2012 and 2013)	{Has signed and/or ratified (or acceded to)}	No	No	No
Jordan	Yes	Information Systems Crime Law of 2010	No	{Has signed and/or ratified (or acceded to)}	No	No
Kazakhstan	Yes	Criminal Code (enacted in 1997 and amended in 2004), Chapter 7. Crimes in the Sphere of Economic Activity (Article 227)	No	No	{Has signed and/or ratified (or acceded to)}	{Has signed and/or ratified (or acceded to)}
Kenya	Yes & Draft Law	▪ Draft Law: Cybercrime and Computer related Crimes Bill, 2014 ▪ Information and Communications Act, 2009 [amended by " Information and Communications (Amendment) Act, 2013"] (Sections 83U to 84F)	No	No	No	No
Kiribati	Yes	Telecommunications Act, 2004 [Part VII – Computer Misuse (Sections 64 to 69)]	No	No	No	No
Korea, Dem. People's Rep.	Yes	Criminal Law (last amended in 2012) (Articles 192, 193, and 194)	No	No	No	No

View citations at the end of this section page 404

C
APPENDIX
TABLE C

National Legal Frameworks on Combating Cybercrime (Assessment Table)

National Legal Frameworks on Combating Cybercrime[1]						
Country Name[2]	Has domestic legislation regarding cybercrime	Name of domestic legislation regarding cybercrime	International or Regional Instrument[3]			
			Budapest Convention	Arab Convention	CIS Agreement	SCO Agreement
Korea, Rep.	Yes	Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. (last amended in 2015) [Chapter X. Penal Provisions (Articles 70 to 76)]	No	No	No	No
Kosovo	Yes	Law on Prevention and Fight of the Cyber Crime, 2010	No	No	No	No
Kuwait	Yes	Law No. 63 of 2015 on combating cyber crimes (effective as of 12 Jan. 2016)	No	{Has signed and/or ratified (or acceded to)}	No	No
Kyrgyz Republic	Yes	Criminal Code (enacted in 1997 and amended in 2006), Chapter 28. Crimes in the Sphere of Computer Information (Articles 289-291)	No	No	{Has signed and/or ratified (or acceded to)}	{Has signed and/or ratified (or acceded to)}
Lao PDR	No		No	No	No	No
Latvia	Yes	Criminal Code (Sections 241 to 245)	{Has signed and/or ratified (or acceded to)}	No	No	No
Lebanon	No		No	No	No	No
Lesotho	Yes & Draft Law	▪ Draft Law: Computer Crime and Cybercrime Bill, 2013 ▪ Penal Code Act, 2010 (Government Gazette: 9 March 2012) [Section 62 (Misuse of property of another), Subsection (2)]	No	No	No	No
Liberia	No		No	No	No	No
Libya	No		No	{Has signed and/or ratified (or acceded to)}	No	No
Liechtenstein	Yes	Criminal Code (*e.g.*, Article 126a, Article 126b)	{Has signed and/or ratified (or acceded to)}	No	No	No

View citations at the end of this section page 404

C
APPENDIX
TABLE C

National Legal Frameworks on Combating Cybercrime (Assessment Table)

National Legal Frameworks on Combating Cybercrime[1]						
Country Name[2]	Has domestic legislation regarding cybercrime	Name of domestic legislation regarding cybercrime	International or Regional Instrument[3]			
			Budapest Convention	Arab Convention	CIS Agreement	SCO Agreement
Lithuania	Yes	▪ Criminal Code (enacted in 2000 and amended in 2010), Chapter 30. Crimes against Security of Electronic Data and Information Systems (Articles 196 to 198(2)) ▪ Criminal Procedure Code	{Has signed and/or ratified (or acceded to)}	No	No	No
Luxembourg	Yes	Penal Code (as amended by Act of 15 Jul. 1993, Law of 14 Aug. 2000, Law of 10 Nov. 2006, and Law of 18 Jul. 2014) (Articles 231bis, 491, and 496, as well as, Section VII.4 – On offences in the field of data processing, Articles 509-1 to 509-7)	{Has signed and/or ratified (or acceded to)}	No	No	No
Macedonia, FYR	Yes	Criminal Code (*e.g.*, Article 251. Damage and unauthorized entering in a computer system)	{Has signed and/or ratified (or acceded to)}	No	No	No
Madagascar	Yes	Act 2014-006 on the fight against cybercrime	No	No	No	No
Malawi	No & Draft Law	▪ Electronic Transactions Bill, 2015, Part X –Offences (Sections 86 to 98) ▪ E-Bill, 2012, Part V-Security in Digital Economy, Chapter 2-Cyber criminality, Sections 42 to 44	No	No	No	No
Malaysia	Yes	Computer Crimes Act, 1997 (incorporating all amendments up to 2006)	No	No	No	No
Maldives	No		No	No	No	No
Mali	Yes	Penal Code (Articles 264 to 271)	No	No	No	No
Malta	Yes	Criminal Code (Chapter 9) (Articles 337B to 337G)	{Has signed and/or ratified (or acceded to)}	No	No	No
Marshall Islands	No		No	No	No	No

View citations at the end of this section page 404

C
APPENDIX
TABLE C

National Legal Frameworks on Combating Cybercrime (Assessment Table)

National Legal Frameworks on Combating Cybercrime[1]						
Country Name[2]	Has domestic legislation regarding cybercrime	Name of domestic legislation regarding cybercrime	International or Regional Instrument[3]			
			Budapest Convention	Arab Convention	CIS Agreement	SCO Agreement
Mauritania	No & Draft Law	Draft Law: Bill on Cybercrime	No	{Has signed and/or ratified (or acceded to)}	No	No
Mauritius	Yes	Computer Misuse and Cybercrime Act, 2003 (Act No. 22 of 2003)	{Has signed and/or ratified (or acceded to)}	No	No	No
Mexico	Yes	Federal Criminal Code (Articles 211bis 1 to Articles 211bis 7)	Invited to accede	No	No	No
Micronesia, Fed. Sts.	No		No	No	No	No
Moldova	Yes	Criminal Code (enacted in 2002 and amended in 2009), Chapter XI. Computer Crimes and Crimes in the Telecommunications Sphere (Articles 259-2611)	{Has signed and/or ratified (or acceded to)}	No	{Has signed and/or ratified (or acceded to)}	No
Monaco	Yes	Law on Digital Economy	{Has signed and/or ratified (or acceded to)}	No	No	No
Mongolia	Yes	Criminal Code (Enacted in 2002) [Special Part, Title 8. Crimes against Public Security and Health, Chapter 25: Crimes against the security of computer data (Articles 226 to 229)]	No	No	No	No
Montenegro	Yes	▪ Criminal Code, Chapter 28. Criminal Acts against Safety of Computer Data (Articles 349 to 356) ▪ Criminal Procedure Code	{Has signed and/or ratified (or acceded to)}	No	No	No
Morocco	Yes	Penal Code (Articles 607-3 to 607-10)	Invited to accede	{Has signed and/or ratified (or acceded to)}	No	No
Mozambique	No		No	No	No	No
Myanmar	Yes	Electronic Transactions Law, 2004 (Articles 2, 34, 38)	No	No	No	No

View citations at the end of this section page 404

C
APPENDIX
TABLE C

National Legal Frameworks on Combating Cybercrime (Assessment Table)

National Legal Frameworks on Combating Cybercrime[1]						
Country Name[2]	Has domestic legislation regarding cybercrime	Name of domestic legislation regarding cybercrime	International or Regional Instrument[3]			
			Budapest Convention	Arab Convention	CIS Agreement	SCO Agreement
Namibia	No & Draft Law	Draft Law: Electronic Communication and Cybercrime Bill	No	No	No	No
Nauru	No		No	No	No	No
Nepal	Yes	Electronic Transaction Act, 2008, Chapter 9. Offense relating to Computer (Sections 44-59)	No	No	No	No
Netherlands	Yes	Criminal Code (*e.g.*, Art. 138ab and Art. 138b)	{Has signed and/or ratified (or acceded to)}	No	No	No
New Zealand	Yes	Crimes Act 1961 (amended by Crimes Amendment Act, 2003) (Articles 248-254)	No	No	No	No
Nicaragua	Yes	Penal Code (*e.g.*, Article 198)	No	No	No	No
Niger	Yes	Penal Code, Title VII. Offences in the Field of Computers (Articles 399.2 to 399.9)	No	No	No	No
Nigeria	Yes	Cybercrimes (Prohibition, Prevention, etc.) Act, 2015	No	No	No	No
Norway	Yes	General Civil Penal Code (Penal Code) (*e.g.*, Sections 145 to 146)	{Has signed and/or ratified (or acceded to)}	No	No	No
Oman	Yes	Royal Decree No. 12 of 2011 Issuing the Cyber Crime Law	No	{Has signed and/or ratified (or acceded to)}	No	No
Pakistan	Yes & Draft Law	▪ Draft Law: Bill - Prevention of Electronic Crimes Act, 2015 ▪ Prevention of Electronic Crime Ordinance, 2009 ▪ Electronic Transactions Ordinance 2002 (Sections 36 to 37)	No	No	No	No
Palau	No		No	No	No	No

View citations at the end of this section page 404

C
APPENDIX
TABLE C

National Legal Frameworks on Combating Cybercrime (Assessment Table)

National Legal Frameworks on Combating Cybercrime[1]						
Country Name[2]	Has domestic legislation regarding cybercrime	Name of domestic legislation regarding cybercrime	International or Regional Instrument[3]			
			Budapest Convention	Arab Convention	CIS Agreement	SCO Agreement
Panama	Yes	Penal Code (approved by Law No. 14 of 2007, with amendments and additions introduced by Law No. 26 of 2008, Law No. 5 of 2009, and Law No. 14 of 2010) (Articles 289 to 292)	{Has signed and/or ratified (or acceded to)}	No	No	No
Papua New Guinea	No		No	No	No	No
Paraguay	Yes	Penal Code (amended by Law No. 4439 of 2011 amending the Penal Code) [*e.g.*, Article 174b (Unauthorized Access to Computer Systems)]	Invited to accede	No	No	No
Peru	Yes	▪ Law No. 30096 of 2013 (Computer Crimes Act) ▪ Law 30171 of 2014 [Law amending the Law No. 30096 of 2013 (Computer Crimes Act)]	Invited to accede	No	No	No
Philippines	Yes	Cybercrime Prevention Act of 2012(Republic Act No. 10175 of 2012)	Invited to accede	No	No	No
Poland	Yes	Penal Code (Articles 267, 268 and 269)	{Has signed and/or ratified (or acceded to)}	No	No	No
Portugal	Yes	Law No. 109/2009, of September 15 (Cybercrime Law)	{Has signed and/or ratified (or acceded to)}	No	No	No
Qatar	Yes	Cybercrime Prevention Law (Law No. 14 of 2014)	No	{Has signed and/or ratified (or acceded to)}	No	No
Romania	Yes	Law on Certain Steps for Assuring Transparency in Performing High Official Positions, Public and Business Positions, for Prevention and Sanctioning the Corruption (Law No. 161/2003) (Anti-Corruption Law) , Title III Preventing and Fighting Cyber Crime (Articles 34 to 67)	{Has signed and/or ratified (or acceded to)}	No	No	No
Russian Federation	Yes	Criminal Code (enacted in 1996 and amended in 2012), Section IX. Crimes Against Public Security and Public Order, Chapter 28. Crimes in the Sphere of Computer Information (Articles 272, 273, and 274)	No	No	{Has signed and/or ratified (or acceded to)}	{Has signed and/or ratified (or acceded to)}

View citations at the end of this section page 404

C
APPENDIX
TABLE C

National Legal Frameworks on Combating Cybercrime (Assessment Table)

National Legal Frameworks on Combating Cybercrime[1]						
Country Name[2]	Has domestic legislation regarding cybercrime	Name of domestic legislation regarding cybercrime	International or Regional Instrument[3]			
			Budapest Convention	Arab Convention	CIS Agreement	SCO Agreement
Rwanda	Yes	▪ Organic Law instituting the Penal Code (No. 01/2012/OL of 02/05/2012), Section 5: Theft committed by use of computers or other similar devices (Articles 306 to 315) ▪ Law Relating to Electronic Messages, Electronic Signatures and Electronic Transactions (No. 18/2010 of 12/05/2010), Chapter 9: Computer Misuse and Cyber Crime (Articles 58 to 65)	No	No	No	No
Samoa	Yes	Crimes Act (No 10. of 2013), Part 18. Crimes involving Electronic Systems (Sections 205 to 220)	No	No	No	No
San Marino	Yes	▪ Law No. 70 of 1995, Rules Concerning the Processing of Personal Data related to Information Technology (Article 17) ▪ Penal Code (Articles 402 and 403)	No	No	No	No
Sao Tome and Principe	No		No	No	No	No
Saudi Arabia	Yes	Anti-Cyber Crime Law (2007)	No	{Has signed and/or ratified (or acceded to)}	No	No
Senegal	Yes	Penal Code (as amended by Law No. 2008-11 on Cybercrime) (Arts. 431-7 to 431-63; 677-34 to 677-42)	{Has signed and/or ratified (or acceded to)}	No	No	No
Serbia	Yes	Criminal Code, Chapter 27. Criminal Offense against Security of Computer Data (Articles 298-304a)	{Has signed and/or ratified (or acceded to)}	No	No	No
Seychelles	Yes	Computer Misuse Act [enacted by Computer Misuse Act (Act No. 17 of 1998) and amended by Computer Misuse (Amendment) Act (Act No. 6 of 2012)]	No	No	No	No
Sierra Leone	No		No	No	No	No
Singapore	Yes	Computer Misuse and Cybersecurity Act (Chapter 50A)	No	No	No	No

View citations at the end of this section page 404

C
APPENDIX
TABLE C

National Legal Frameworks on Combating Cybercrime (Assessment Table)

National Legal Frameworks on Combating Cybercrime[1]						
Country Name[2]	Has domestic legislation regarding cybercrime	Name of domestic legislation regarding cybercrime	International or Regional Instrument[3]			
			Budapest Convention	Arab Convention	CIS Agreement	SCO Agreement
Slovak Republic	Yes	Criminal Code (Law No. 300 of 2005) [*e.g.*, Section 247 (Harm Done to and Abuse of an Information Carrier)]	{Has signed and/or ratified (or acceded to)}	No	No	No
Slovenia	Yes	Penal Code [*e.g.*, Article 225 (Unauthorized Access to an Information System)]	{Has signed and/or ratified (or acceded to)}	No	No	No
Solomon Islands	No		No	No	No	No
Somalia	No		No	No	No	No
South Africa	Yes & Draft Law	▪ Electronic Communications and Transactions Act, 2002 (No. 25 of 2002), Chapter 8: Cybercrime (Sections 85-89) ▪ Cybercrimes Bill, 2015	{Has signed and/or ratified (or acceded to)}	No	No	No
South Sudan	Yes	Penal Code Act, 2008, Chapter 27. Computer and Electronic Related Offenses (Sections 388 to 394)	No	No	No	No
Spain	Yes	Criminal Code (*e.g.*, Article 197)	{Has signed and/or ratified (or acceded to)}	No	No	No
Sri Lanka	Yes	Computer Crime Act (also known as " Computer Crimes Act"), (No. 24 of 2007)	{Has signed and/or ratified (or acceded to)}	No	No	No
St. Kitts and Nevis	Yes	Electronic Crimes Act, 2009	No	No	No	No
St. Lucia	No & Draft Law	Draft Law: Electronic Crimes Bill, 2009	No	No	No	No
St. Vincent and the Grenadines	Yes	Electronic Transactions Act, 2007, Part X. Information Systems and Computer Related Crimes (Sections 64 to 73)	No	No	No	No
Sudan	Yes	The Informatic Offences (Combating) Act, 2007	No	{Has signed and/or ratified (or acceded to)}	No	No

View citations at the end of this section page 404

C
APPENDIX
TABLE C

National Legal Frameworks on Combating Cybercrime (Assessment Table)

National Legal Frameworks on Combating Cybercrime[1]						
Country Name[2]	Has domestic legislation regarding cybercrime	Name of domestic legislation regarding cybercrime	International or Regional Instrument[3]			
			Budapest Convention	Arab Convention	CIS Agreement	SCO Agreement
Suriname	No & Draft Law	▪ Bill of the First Book of the Criminal Code (2006) ▪ Bill of the Second Book of the Criminal Code (2009) (*e.g.*, Articles 187g, 213C, and 414a)	No	No	No	No
Swaziland	No & Draft Law	Draft Law: Computer Crime and Cybercrime Bill, 2013	No	No	No	No
Sweden	Yes	Penal Code, Chapter 4, Section 9 c	{Has signed and/or ratified (or acceded to)}	No	No	No
Switzerland	Yes	Penal Code (Articles 143bis &144bis)	{Has signed and/or ratified (or acceded to)}	No	No	No
Syrian Arab Republic	Yes	Law for the Regulation of Network Communication Against Cyber Crime, 2012 (also called "Law on the network communication and computer crime control, 2012")	No	{Has signed and/or ratified (or acceded to)}	No	No
Tajikistan	Yes	Criminal Code (enacted in May 21, 1998), Section XII. Crimes against Information Security, Chapter 28. Crimes against Information Security (Articles 298-304)	No	No	{Has signed and/or ratified (or acceded to)}	{Has signed and/or ratified (or acceded to)}
Tanzania	Yes	Cybercrimes Act, 2015	No	No	No	No
Thailand	Yes	Computer Crime Act, 2007	No	No	No	No
Timor-Leste	No		No	No	No	No
Togo	No & Draft Law	The Draft Law on the Fight against Cybercrime	No	No	No	No
Tonga	Yes	Computer Crimes Act (Act No. 14 of 2003)	{Has signed and/or ratified (or acceded to)}	No	No	No

View citations at the end of this section page 404

C
APPENDIX
TABLE C

National Legal Frameworks on Combating Cybercrime (Assessment Table)

National Legal Frameworks on Combating Cybercrime[1]						
Country Name[2]	Has domestic legislation regarding cybercrime	Name of domestic legislation regarding cybercrime	International or Regional Instrument[3]			
			Budapest Convention	Arab Convention	CIS Agreement	SCO Agreement
Trinidad and Tobago	Yes & Draft Law	▪ Computer Misuse Act, 2000 ▪ Draft Law: The Cybercrime Bill, 2015	No	No	No	No
Tunisia	Yes & Draft Law	▪ Draft Law: Cybercrime Bill, 2014 ▪ Penal Law (Articles 199 bis and 199ter)	No	{Has signed and/or ratified (or acceded to)}	No	No
Turkey	Yes	▪ Criminal Code (10th Section. Offences in the field of Data Processing Systems. Articles 243 to 246) ▪ Law No. 5651 on Regulation of Internet Publications and Combating Crimes Committed through such Publications, 2007 (amended by Law No. 6518 of 2014) ▪ Regulation on the Principles and Procedures of Regulating the Publications on the Internet	{Has signed and/or ratified (or acceded to)}	No	No	No
Turkmenistan	Yes	Criminal Code (enacted in 1997, entered into force in 1998, and last amended in 2014), Chapter 33. Computer Information Crimes (Articles 333 to 335)	No	No	No	No
Tuvalu	No		No	No	No	No
Uganda	Yes	Computer Misuse Act, 2011	No	No	No	No
Ukraine	Yes & Draft Law	▪ Draft Law on Combating Cybercrime, 2014 ▪ Criminal Code (enacted in 2001 and amended in 2005), Chapter XVI. Criminal Offenses related to the Use of Electronic Computing Machines (Computers), Systems and Computer Networks and Telecommunication Networks (Articles 361 to 363-1)	{Has signed and/or ratified (or acceded to)}	No	{Has signed and/or ratified (or acceded to)}	No
United Arab Emirates	Yes	Federal Decree-Law No. 5 of 2012 on Combating Cyber Crimes (replacing Federal Law No. 2 of 2006 on the Prevention of Information Technology Crimes)	No	{Has signed and/or ratified (or acceded to)}	No	No

View citations at the end of this section page 404

C
APPENDIX
TABLE C

National Legal Frameworks on Combating Cybercrime (Assessment Table)

National Legal Frameworks on Combating Cybercrime[1]						
Country Name[2]	Has domestic legislation regarding cybercrime	Name of domestic legislation regarding cybercrime	International or Regional Instrument[3]			
			Budapest Convention	Arab Convention	CIS Agreement	SCO Agreement
United Kingdom	Yes	▪ Computer Misuse Act, 1990 (last amended by Serious Crimes Act, 2015) ▪ Regulations of Investigatory Powers Act, 2000	{Has signed and/or ratified (or acceded to)}	No	No	No
United States	Yes	▪ 15 (Title 15) U.S.C. (United States Code), Chapter 103 - Controlling the Assault of Non-solicited Pornography and Marketing , § (Section) 7701-7713 ▪ 18 U.S.C., Chapter 47-Crimes and Criminal Procedure, § 1028 through 1030; Chapter 119 - Wire and Electronic Communications Interception and Interception of Oral Communications; Chapter 121 - Stored Wire and Electronic Communications and Transactional Record Access; and §3121, General prohibition on pen register and trap and trace device use; exception	{Has signed and/or ratified (or acceded to)}	No	No	No
Uruguay	Yes	Penal Code [Enacted by Law No. 9,155 of 1933 and Amended by Law No. 18,383 of 2008 (Attack on the regularity of telecommunications)] (*e.g.*, Article 217)	No	No	No	No
Uzbekistan	Yes	Criminal Code (enacted in 1994, came into force in 1995, and amended in 2001), Special Part, Section III. Economic Crimes, Chapter 11. Crimes unrelated to Larceny of Property (Article 174: Computer-related Crimes)	No	No	{Has signed and/or ratified (or acceded to)}	{Has signed and/or ratified (or acceded to)}
Vanuatu	No		No	No	No	No
Venezuela, RB	Yes	Special Law against Computer Crimes, 2001	No	No	No	No
Vietnam	Yes	▪ Law on information technology (Law No. 67/2006/QH11) ▪ Penal Code (Enacted by Law No. 15/1999/QH10 and Amended by Law No. 37/2009/QH12) (*e.g.*, Article 226a)	No	No	No	No

View citations at the end of this section page 404

C
APPENDIX
TABLE C

National Legal Frameworks on Combating Cybercrime (Assessment Table)

National Legal Frameworks on Combating Cybercrime[1]						
Country Name[2]	Has domestic legislation regarding cybercrime	Name of domestic legislation regarding cybercrime	International or Regional Instrument[3]			
			Budapest Convention	Arab Convention	CIS Agreement	SCO Agreement
West Bank and Gaza	No & Draft Law	Draft Penal Code (Part 12. Cybercrimes, Articles 646 to 677)	No	{Has signed and/or ratified (or acceded to)}	No	No
Yemen, Rep.	No & Draft Law	Draft law for combating electronic crimes (also called "Draft Law on Combating Electronic Crime")	No	{Has signed and/or ratified (or acceded to)}	No	No
Zambia	Yes	▪ Computer Misuse and Crimes Act, 2004 (No. 13 of 2004) ▪ Electronic Communication and Transactions Act, 2009 (No. 21 of 2009) [Part XIV. Cyber Inspectors (Sections 93 to 97), Part XV. Cyber Crimes (Sections 98 to 109)]	No	No	No	No
Zimbabwe	Yes & Draft Law	▪ Computer Crime and Cybercrime Bill ▪ Criminal Law (Codification and Reform) Act, Chapter VIII. Computer-related Crimes (Sections 162-168)	No	No	No	No

View citations at the end of this section page 404

D
APPENDIX
TABLE D1

Comparative Analysis of Indicators Used in In-Country Assessment Tools

Explanatory Note: The Project reviewed the in-country assessment tools used developed by participants in this Project. The indicators developed (in the left-hand column) are a synthesis of those assessments, as well as other assessments. The synthesized set of indicator were then "mapped" against the respective tools. Where an assessment includes an indicator, it is indicated with a "Y", as well as where in the particular assessment, the indicator can be found or is referenced. In cases where an assessment explicitly stated that its questions were prepared corresponding to provisions of an exogenous reference (*e.g.*, a particular multilateral instrument or a sample legislative language) the indicators were considered in light of those corresponding. The frequency with which an indicator appears in the assessments is shown in the right-hand column. The color-coding for frequency is shown at the bottom of the table. More information about the assessments may be found in the endnotes to this Appendix. The synthesized indicators shown here also formed the basis of the Assessment Tool developed by this Project and included in appendix 9.

Non-Legal Frameworks						
In-Country Assessment Tools / Indicators	**AIDP[1]**	**CoE[2]**	**ITU[3]**	**UNODC Cybercrime Questionnaire (2012)[4] & Comprehensive Study[5]**	**Oxford[6]**	**Frequency** Number of Entities Covered (out of 5)
Non-Legal Frameworks	Y (Page 5)			Y (2012) [**a.**Q1 to Q11, **b.**Q113 to Q120, **c.**Q15 to Q164, **d.**Q186 to 192, **e.**Q241 to 261]	Y (Pages 29 to 32)	**3 of 5**
1. National strategy (or "national policy") on cybercrime				Y (2012) (Q1)		**1 of 5**
a. Binding all relevant authorities and private sector						**0 of 5**
i. Binding public-private						**0 of 5**
ii. Binding public						**0 of 5**
iii. No binding force						**0 of 5**
b. Long term strategy?						**0 of 5**
i. Longer than 5 years						**0 of 5**
ii. Longer than 3 years						**0 of 5**
iii. Less than 3 years						**0 of 5**
iv. No specific term						**0 of 5**
c. Define specific vulnerable areas to be protected						**0 of 5**

View citations at the end of this section page 405

D
APPENDIX
TABLE D1

Comparative Analysis of Indicators Used in In-Country Assessment Tools

Continued from last page

Non-Legal Frameworks						
In-Country Assessment Tools / Indicators	**AIDP[1]**	**CoE[2]**	**ITU[3]**	**UNODC Cybercrime Questionnaire (2012)[4] & Comprehensive Study[5]**	**Oxford[6]**	**Frequency** Number of Entities Covered (out of 5)
d. Define resources and necessities to fight cybercrime						**0 of 5**
i. Human resource (HR)						**0 of 5**
ii. Assets including devices & infrastructure						**0 of 5**
iii. User protection strategy						**0 of 5**
2. Define lead government institution responsible for coordinating the prevention and combating cybercrime				Y (2012) (Q2)		**1 of 5**
a. Higher than PM						**0 of 5**
b. Ministerial level						**0 of 5**
c. Lower than ministerial level						**0 of 5**
3. PPPs to obtain information and evidence from the private sector (*e.g.*, service providers)				Y (2012) (Q6)		**1 of 5**
a. Formal cooperation with the private sector (*e.g.*, service providers)				Y (2012) (Q102), Y (2013) (Page 146)		**1 of 5**
i. By court order				Y (2012) (Q102), Y (2013) (Page 146)		**1 of 5**
ii. By prosecution order				Y (2012) (Q102), Y (2013) (Page 146)		**1 of 5**
iii. By police letter				Y (2012) (Q102), Y (2013) (Page 146)		**1 of 5**
b. Informal cooperation with the private sector (*e.g.*, service providers)				Y (2012) (Q103)		**1 of 5**
4. Maintain statistics on cybercrime	Y (Page 5)			Y (2012) (**a.**Q10, **b.**Q54 to 71, **c.**Q121 to Q138, **d.**Q165 to Q182)	Y (Pages 29 to 32)	**3 of 5**

View citations at the end of this section page 405

D
APPENDIX
TABLE D1

Comparative Analysis of Indicators Used in In-Country Assessment Tools

Continued from last page

Non-Legal Frameworks						
In-Country Assessment Tools / Indicators	**AIDP[1]**	**CoE[2]**	**ITU[3]**	**UNODC Cybercrime Questionnaire (2012)[4] & Comprehensive Study[5]**	**Oxford[6]**	**Frequency** Number of Entities Covered (out of 5)
a. Designated authority to collect & analyze statistics on cybercrime						**0 of 5**
b. Define statistics necessary for cybercrime						**0 of 5**
c. Updates to statistics on cybercrime regularly						**0 of 5**
5. Technical cooperation on cybercrime				Y (2012) (Q241 to Q261)		**1 of 5**

View citations at the end of this section page 405

D
APPENDIX
TABLE D2

Comparative Analysis of Indicators Used in In-Country Assessment Tools

Legal Frameworks						
In-Country Assessment Tools / Indicators	**AIDP**	**CoE**	**ITU**	**UNODC Cybercrime Questionnaire & Comprehensive Study**	**Oxford**	**Frequency** Number of Entities Covered (out of 5)
National Legal Frameworks	Y (Pages 1 to 5)	Y (Arts. 1 to 35)	Y (Q1 to Q34)	Y (Q12 to Q53)	Y (Pages 27 to 28)	**5 of 5**
1. Domestic legislation regarding cybercrime	Y (Pages 1 to 5)	Y (Arts. 1 to 35)	Y (Q1 to Q34)	Y (Q12 to Q53)	Y (Pages 27 to 28)	**5 of 5**
a. Is cybercrime regulated by law	Y (Page 1) [(…) criminal laws related to cyber-crimes (…)]	Y (Page 1) [Corresponding provisions (…) in national legislation]	Y (Page 35) (Citation of provision, Consistent with Toolkit)	Y (Q12) [(…) main legislation that is specific to cybercrime (…)]	Y (Pages 27 to 28) (Substantive cybercrime law, Procedural cybercrime law)	**5 of 5**
i. Comprehensively Yes						**0 of 5**
ii. Partially Yes with draft law						**0 of 5**
iii. Partially Yes without draft law						**0 of 5**
iv. No (no enacted law) but draft law						**0 of 5**
b. Have detailed definitions of the terms related cybercrime		Y (Art.1)	Y (Q1)			**2 of 5**
i. Computer data		Y (Art. 1 – "computer data")	Y (Q1.c.)			**2 of 5**
ii. Computer system		Y (Art. 1 – "computer system")	Y (Q1.e.)			**2 of 5**
iii. Service provider		Y (Art. 1 – "service provider")	Y (Q1.p.)			**2 of 5**
iv. Subscriber information		Y (Art. 18, – Ex. Rept. 177-180)	Y (Q1.q.)			**1 of 5**
v. Traffic data		Y (Art. 1 – "traffic data")	Y (Q1.r.)			**2 of 5**
2. Multilateral treaties on cybercrime		Y (Page 1)			Y (Pages 27 to 28)	**2 of 5**
a. Signature		Y (Page 1)			Y (Page 27)	**2 of 5**
b. Ratification (or "accession")		Y (Page 1)			Y (Pages 27 to 28)	**2 of 5**

View citations at the end of this section page 405

D
APPENDIX
TABLE D3

Comparative Analysis of Indicators Used in In-Country Assessment Tools

Substantive Law						
In-Country Assessment Tools / Indicators	**AIDP**	**CoE**	**ITU**	**UNODC Cybercrime Questionnaire & Comprehensive Study**	**Oxford**	**Frequency** Number of Entities Covered (out of 5)
Substantive Law	Y (2013) (Pages 1 to 5)	Y (Arts. 2 to 12)	Y (Q2 to Q11)	Y (Q25 to Q40)	Y (Pages 27 to 28)	**5 of 5**
1. Criminalization of offences directed against the confidentiality, integrity, and availability of computer data or systems	Y (2013) (Pages 1 to 2)	Y (Arts. 2 to 6)	Y (Q2 to Q6)	Y (Q25 to Q29)		**4 of 5**
a. Illegal access to a computer system	Y (2013) (Page 1)	Y (Art 2.)	Y (Q2)	Y(Q25)		**4 of 5**
b. Illegal interception	Y (2013) (Page 1)	Y (Art. 3)	Y (Q5)	Y (Q26)		**4 of 5**
c. Data interference	Y (2013) (Page 1)	Y (Art. 4)	Y (Q4, b.)	Y (Q27)		**4 of 5**
d. System interference	Y (2013) (Page 1)	Y(Art. 5)	Y (Q4, a.)	Y (Q27)		**4 of 5**
e. Misuse of devices	Y (2013) (Page 2)	Y(Art. 6)	Y (Q6)	Y (Q28)		**4 of 5**
2. Criminalization of traditional offences committed by/through the use of computer systems or data	Y (2013) (Pages 2 to 4)	Y (Arts. 7 to 10)	Y (Q7, and Q8)	Y (Q30 to Q32, Q34 to Q38)		**4 of 5**
a. Computer-related forgery	Y (2013) (Page 2)	Y (Art. 7)	Y (Q7)	Y (Q30)		**4 of 5**
b. Computer-related fraud	Y (2013) (Page 4)	Y (Art. 8)	Y (Q8)	Y (Q30)		**4 of 5**
c. Computer-related copyright and trademark offences	Y (2013) (Page 4)	Y (Art. 10)		Y (Q32)		**3 of 5**
d. Computer-related identity offences	Y (2013) (Page 3)	Y (Arts. 2-8)		Y (Q31)		**2 of 5**
e. Computer-related child pornography offences	Y (2013) (Pages 3 to 4)	Y (Art. 9)		Y (Q36)		**3 of 5**

View citations at the end of this section page 405

D
APPENDIX
TABLE D3

Comparative Analysis of Indicators Used in In-Country Assessment Tools

Continued from last page

Substantive Law						
In-Country Assessment Tools / Indicators	**AIDP**	**CoE**	**ITU**	**UNODC Cybercrime Questionnaire & Comprehensive Study**	**Oxford**	**Frequency** Number of Entities Covered (out of 5)
3. Corporate liability		Y (Art. 12)	Y (Q11)	Y (Q40)		**3 of 5**
4. Aid, abet or attempt						
a. Aid or abet		Y (Art. 11)	Y (Q10)			**4 of 5**
b. Attempt		Y (Art. 11)	Y (Q10)	Y (Q40)		**3 of 5**

View citations at the end of this section page 405

D
APPENDIX
TABLE D4

Comparative Analysis of Indicators Used in In-Country Assessment Tools

Procedural Law						
In-Country Assessment Tools / Indicators	**AIDP**	**CoE**	**ITU**	**UNODC Cybercrime Questionnaire & Comprehensive Study**	**Oxford**	**Frequency** Number of Entities Covered (out of 5)
Procedural Law	Y (Pages 1 to 2)	Y (Arts. 14 to 21)	Y (Q12 to Q20)	Y (Q42 to Q53)	Y (Page 28)	**5 of 5**
1. Scope of procedural provisions		Y (Art. 14)	Y (Q12			**2 of 5**
2. Procedural conditions & safeguards		Y (Art. 15)	Y (Q13)			**2 of 5**
3. Expedited Preservation of stored computer data (data preservation)		Y (Art. 16)	Y (Q14)	Y (Q49)		**3 of 5**
4. Expedited preservation & partial disclosure of traffic data		Y (Art. 17)	Y (Q15)	Y (Q45)		**3 of 5**
5. Expedited preservation of computers or storage media[7]			Y (Q16)			**1 of 5**
6. Production Order						
a. Production order: Specified computer data		Y (Art. 18)	Y (Q17)			**2 of 5**
b. Production order: Subscriber information		Y (Art. 18)	Y (Q17)	Y (Q44)		**3 of 5**
7. Search & seizure of computer data and/or computer systems	Y (Page 1)	Y (Art. 19)	Y (Q18)	Y (Q42, Q43)		**4 of 5**
8. Real-time collection of traffic data	Y (Page 1)	Y (Art.20)	Y (Q19)	Y (Q47)		**4 of 5**
9. Interception of content data	Y (Page 1)	Y (Art. 21)	Y (Q20)	Y (Q48)		**4 of 5**
10. Use of remote forensic tools				Y (Q50)		**1 of 5**
11. Trans-border access to computer data		Y (Art. 32)		Y (Q51)		**1 of 5**

View citations at the end of this section page 405

Comparative Analysis of Indicators Used in In-Country Assessment Tools

Continued from last page

Procedural Law						
In-Country Assessment Tools / Indicators	**AIDP**	**CoE**	**ITU**	**UNODC Cybercrime Questionnaire & Comprehensive Study**	**Oxford**	**Frequency** Number of Entities Covered (out of 5)
12. Obtaining information and evidence from third parties						
a. Compelling third parties (non-targets) to provide information				Y (Q101)		**1 of 5**
b. Compelling private actors (*e.g.*, service providers) to provide information	Y (Page 1)	Y (Arts. 18-21)				**1 of 5**
(2) Private actors (*e.g.*, service providers)' voluntary provision (supply) of information	Y (Page 1)					**1 of 5**

View citations at the end of this section page 405

Comparative Analysis of Indicators Used in In-Country Assessment Tools

Electronic Evidence						
In-Country Assessment Tools / Indicators	**AIDP**	**CoE**	**ITU**	**UNODC Cybercrime Questionnaire & Comprehensive Study**	**Oxford**	**Frequency** Number of Entities Covered (out of 5)
e-Evidence	Y (Page 2)			Y (2012) (Q111, Q105, Q144 to Q147), Y (2013) (Pages 157 to 182)	Y (Pages 29 to 32)	**3 of 5**
1. Rules on e-evidence						
(1) Rules on admissibility of e-evidence	Y (Page 2)			Y (2012) (2012) (Q144)		**2 of 5**
(2) Rules on admissibility of e-evidence obtained from foreign jurisdictions				Y (2012) (Q145)		**1 of 5**
(3) Rules on discovery of e-evidence	Y (Page 2)					**1 of 5**
(4) Rules on evaluating (probative value of) e-evidence	Y (Page 2)					**1 of 5**
(5) Other rules specific to e-evidence	Y (Page 2)			Y (2012) (Q146)		**2 of 5**
2. Law enforcement and Electronic Evidence						
(1) Collecting e-evidence with integrity	Y (Page 2)			Y (2012) (Q111)		**2 of 5**
(2) Storing/retaining e-evidence	Y (Page 2)			Y (2012) (Q111)		**2 of 5**
(3) Transferring e-evidence to courts or prosecutors from law enforcement agencies				Y (2012) (Q111)		**1 of 5**
(4) Obtaining e-evidence in foreign jurisdictions				Y (2012) (Q105), Y (2013) (Page 201)		**1 of 5**
1) Formal MLA request		Y (Arts. 27 to 28, 31)		Y (2012) (Q105), Y (2013) (Page 201)		**1 of 5**

View citations at the end of this section page 405

Comparative Analysis of Indicators Used in In-Country Assessment Tools

Continued from last page

Electronic Evidence						
In-Country Assessment Tools / Indicators	**AIDP**	**CoE**	**ITU**	**UNODC Cybercrime Questionnaire & Comprehensive Study**	**Oxford**	**Frequency** Number of Entities Covered (out of 5)
2) Informal police cooperation				Y (2012) (Q105), Y (2013) (Page 201)		**1 of 5**
3) Direct contact with service providers				Y (2012) (Q105), Y (2013) (Page 201)		**1 of 5**
4) 24/7 network		Y (Arts. 35)		Y (2012) (Q105), Y (2013) (Page 201)		**1 of 5**
5) Other (please specify)		Y (Arts. 26, 29, 30, 32 to 34) (respectively spontaneous information, preservation, expedited disclosure, transborder search, real-time traffic collection, real-time interception)		Y (2012) (Q105), Y (2013) (Page 201)		**1 of 5**

View citations at the end of this section page 405

D
APPENDIX
TABLE D6

Comparative Analysis of Indicators Used in In-Country Assessment Tools

Jurisdiction						
In-Country Assessment Tools / Indicators	**AIDP**	**CoE**	**ITU**	**UNODC Cybercrime Questionnaire & Comprehensive Study**	**Oxford**	**Frequency** Number of Entities Covered (out of 5)
Jurisdiction	Y (Page 1)	Y (Art. 22)	Y (Q21)	Y (2012) (Q18 to Q19), Y (2013) (Pages 191 to 196)		**4 of 5**
1. Common national bases for jurisdiction over cybercrime acts						
(1) Territory basis						
1) Offence is committed (partly or wholly) within its territory		Y (Art. 22)	Y (Q21.a.)	Y (2012) (Q18), Y (2013) (Page 191)		**2 of 5**
2) Offence is committed using a computer system or data located within its territory		Y (Art. 22)		Y (2012) (Q18), Y (2013) (Page 192)		**1 of 5**
3) Offence is directed against a computer system or data within its territory		Y (Art. 22)		Y (2012) (Q18), Y (2013) (Page 192)		**1 of 5**
4) Effect or damage of the offence is located within its territory				Y (2012) (Q18), Y (2013) (Page 191)		**1 of 5**
5) Offence is committed on a ship or aircraft registered to your country		Y (Art. 22)	Y (Q21.b)			**1 of 5**
(2) Nationality-basis						
1) Nationality of the offender		Y (Art. 22)	Y (Q21.c.)	Y (2012) (Q18), Y (2013) (Page 191)		**2 of 5**
2) Nationality of the victim				Y (2012) (Q18), Y (2013) (Page 191)		**1 of 5**
2. Jurisdiction where extradition refused		Y (Art. 22)	Y (Q21.d.)			**1 of 5**
3. Concurrent jurisdiction (conflicts of jurisdiction)	Y (Page 1)	Y (Art. 22)	Y (Q21.e.)	Y (2012) (Q18)		**3 of 5**

View citations at the end of this section page 405

D
APPENDIX
TABLE D6

Comparative Analysis of Indicators Used in In-Country Assessment Tools

Continued from last page

Jurisdiction						
In-Country Assessment Tools / Indicators	**AIDP**	**CoE**	**ITU**	**UNODC Cybercrime Questionnaire & Comprehensive Study**	**Oxford**	**Frequency** Number of Entities Covered (out of 5)
4. Establishment of the place where the offence occurred	Y (Page 1)		Y (Q21.f)			**2 of 5**
5. Dual criminality				Y (2012) (Q18), Y (2013) (Page 194)		**1 of 5**
6. Reservation		Y (Art. 22)	Y (Q21.g.)			**1 of 5**

View citations at the end of this section page 405

D
APPENDIX
TABLE D7

Comparative Analysis of Indicators Used in In-Country Assessment Tools

Legal Safeguards						
In-Country Assessment Tools / Indicators	**AIDP**	**CoE**	**ITU**	**UNODC Cybercrime Questionnaire & Comprehensive Study**	**Oxford**	**Frequency** Number of Entities Covered (out of 5)
Safeguards	Y (2012) (Page 2)	Y (Art. 15)		Y (Q20 to Q24)	Y (Pages 26 to 27)	**3 of 5**
1. Privacy and (personal) data protection		CoE Convention 108		Y (Q21 to Q24)	Y (Pages 26 to 27)	**3 of 5**
2. Freedom of expression	Y (2012) (Page 2)			Y (Q20)	Y (Pages 26)	**3 of 5**

View citations at the end of this section page 405

Comparative Analysis of Indicators Used in In-Country Assessment Tools

International Cooperation						
In-Country Assessment Tools / Indicators	**AIDP**	**CoE**	**ITU**	**UNODC Cybercrime Questionnaire & Comprehensive Study**	**Oxford**	**Frequency** Number of Entities Covered (out of 5)
International Cooperation	Y (Pages 1 to 2)	Y (Arts. 23 to 35)	Y (Q22 to Q33)	Y (2012) (Q193 to Q240)	Y (Pages 29 to 32)	**5 of 5**
1. Formal international cooperation						
a. General principles relating to international cooperation		Y (Art. 23)	Y (Q22)			**2 of 5**
b. General Principles relating to Extradition		Y (Art. 24)	Y (Q23)	Y (2012) (Q193 to Q215)		**3 of 5**
i. Domestic legislation for extradition in cybercrime cases		Y (Art. 24)		Y (2012) (Q 193), Y (2013) (Page 200)		**1 of 5**
ii. Treaty or reciprocity in the absence of treaty provisions		Y (Art. 24)		Y (2012) (Q202 to Q207), Y (2013) (Page 201)		**1 of 5**
iii. Central authority		Y (Art. 24)		Y (2012) (Q195)		**1 of 5**
iv. Refusal of extradition		Y (Art. 24)	Y (Q23.d)			**1 of 5**
v. Dual criminality		Y (Art. 24)		Y (2012) (Q198), Y (2013) (Page 204)		**1 of 5**
vi. Seriousness of a minimum penalty		Y (Art. 24)		Y (2012) (Q198), Y (2013) (Page 204)		**1 of 5**
c. General principles relating to MLA	Y (Page 1)	Y (Art. 25)	Y (Q24)	Y (2012) (Q216 to Q240)		**4 of 5**
i. Domestic legislation for MLA in cybercrime cases		Y (Art. 25)		Y (2012) (Q216), Y (2013) (Page 200)		**1 of 5**
ii. Treaty or reciprocity in the absence of treaty provisions		Y (Art. 27)		Y (2012) (Q227 to Q232), Y (2013) (Page 201)		**1 of 5**
iii. Central Authority		Y (Art. 27)		Y (2012) (Q217)		**1 of 5**

View citations at the end of this section page 405

Comparative Analysis of Indicators Used in In-Country Assessment Tools

Continued from last page

International Cooperation						
In-Country Assessment Tools / Indicators	**AIDP**	**CoE**	**ITU**	**UNODC Cybercrime Questionnaire & Comprehensive Study**	**Oxford**	**Frequency** Number of Entities Covered (out of 5)
iv. Expedited means of communication		Y (Arts. 25 & 27)	Y (Q24.b.)			**1 of 5**
v. Refusal to cooperate or assist	Y (Page 1)	Y (Arts. 25 & 27)	Y (Q24.c, Q26.c)			**2 of 5**
vi. Dual Criminality	Y (Page 1)	Y (Arts. 25)	Y (Q24.d.)	Y (2012) (Q220), Y(2013) (Pages 204 to 205)		**2 of 5**
vii. Confidentiality of information to be provided and limitation on use		Y (Art. 28	Y (Q26.g)			**2 of 5**
viii. Spontaneous (unsolicited) information		Y (Art. 26)	Y (Q25)			**2 of 5**
d. Specific Provisions relating to MLA	Y (Page 1)	Y (Arts. 29 to 34)	Y (Q27 to Q32)	Y (2012) (Q108)		**4 of 5**
i. MLA relating to provisional measures						
(a) Expedited preservation of stored computer data		Y (Art. 29)	Y (Q27)			**2 of 5**
(b) Expedited disclosure of preserved traffic data		Y (Art. 30)	Y (Q28)			**2 of 5**
ii. MLA relating to investigative powers						
(a) MLA regarding accessing of stored computer data		Y (Art. 31)	Y (Q29)			**2 of 5**
(b) Trans-border access to stored computer data		Y (Art.32)	Y (Q30)	Y (2012) (Q108)		**3 of 5**
(c) MLA in the real-time collection of traffic data		Y (Art. 33)	Y (Q31)			**2 of 5**

View citations at the end of this section page 405

Comparative Analysis of Indicators Used in In-Country Assessment Tools

Continued from last page

International Cooperation						
In-Country Assessment Tools / Indicators	**AIDP**	**CoE**	**ITU**	**UNODC Cybercrime Questionnaire & Comprehensive Study**	**Oxford**	**Frequency** Number of Entities Covered (out of 5)
(d) MLA regarding the interception of content data	Y (Page 1)	Y (Art. 34)	Y (Q32)			**3 of 5(**
2. Informal international cooperation						
a. Multilateral network (*e.g.*, 24/7 network)	Y (Page 2)	Y (Art. 35)	Y (Q33)	Y (2012) (Q107)		**4 of 5**
b. Bilateral network (*e.g.*, direct police-to-police cooperation)				Y (2012) (Q106, Q223)		**1 of 5**

View citations at the end of this section page 405

D
APPENDIX
TABLE D9

Comparative Analysis of Indicators Used in In-Country Assessment Tools

Capacity Building						
In-Country Assessment Tools / Indicators	**AIDP**	**CoE**	**ITU**	**UNODC Cybercrime Questionnaire & Comprehensive Study**	**Oxford**	**Frequency** Number of Entities Covered (out of 5)
Capacity-building	Y (Page 5)			Y (**a.**Q113 to Q120, **b.**Q157 to Q164, **c.**Q186 to Q192)	Y (Pages 29 to 32)	**3 of 5**
1. CERT				Y (Q10)		**1 of 5**
2. Law enforcement (police)	Y (Page 5)	Not in the treaty text but extensive ancillary program		Y (Q113 to Q120)	Y (Pages 29 to 30)	**3 of 5**
a. Law enforcement structure for cybercrime cases				Y (Q 113)		**1 of 5**
b. Separate unit/agency specifically for investigating cybercrime	Y (Page 5)			Y (Q114)		**2 of 5**
c. Specialized police officers assigned to cybercrime cases				Y (Q115)		**1 of 5**
d. Sufficient resources and capabilities to investigate cybercrime cases and/or cases involving electronic evidence (including digital forensic tools)					Y (Page 29)	**1 of 5**
e. Training programs to police officers in the investigation of cybercrime cases	Y (Page 5)			Y (Q117 to Q120)	Y (Page 29)	**3 of 5**
3. Prosecution	Y (Page 5)	Not in the treaty text but extensive ancillary program		Y (Q157 to Q164)	Y (Pages 30 to 31)	**3 of 5**
a. Prosecution structure for cybercrime cases				Y (Q157)		**1 of 5**
b. Separate unit/agency specifically for prosecuting cybercrime	Y (Page 5)			Y (Q158)		**2 of 5**

View citations at the end of this section page 405

Comparative Analysis of Indicators Used in In-Country Assessment Tools

Continued from last page

Capacity Building						
In-Country Assessment Tools / Indicators	**AIDP**	**CoE**	**ITU**	**UNODC Cybercrime Questionnaire & Comprehensive Study**	**Oxford**	**Frequency** Number of Entities Covered (out of 5)
c. Specialized prosecutors assigned to cybercrime cases				Y (Q159 to Q163)		**1 of 5**
d. Sufficient resources and capacities to prosecute cybercrime cases and/or cases involving electronic evidence					Y (Page 30)	**1 of 5**
e. Training programs to prosecutors for cybercrime cases	Y (Page 5)			Y (Q161 to Q164)	Y (Page 30)	**3 of 5**
4. Court	Y (Page 5)	Not in the treaty text but extensive ancillary program		Y (Q186 to Q192)	Y (Pages 31 to 32)	**3 of 5**
a. Court structure for cybercrime cases				Y (Q186)		**1 of 5**
b. Separate courts specifically for the trial of cybercrime cases				Y (Q 186 to Q187)		**1 of 5**
c. Specialized judges assigned to cybercrime cases				Y (Q188 to Q191)		**1 of 5**
d. Training programs to judges in the trial of cybercrime cases	Y (Page 5)			Y (Q189 to Q192)	Y (Page 31)	**3 of 5**

View citations at the end of this section page 405

E
APPENDIX
TABLE E

Synthetic In-Country Assessment Tool (Assessment Table)

Explanatory Note: This Table sets forth the Toolkit's synthetic, in-country assessment tool (Assessment Tool), as discussed in chapter 7. The purpose of the Assessment Tool is to enable a user to determine gaps in capacity and to highlight priority areas in directing capacity-building resources. The first use of the Assessment Tool will provide a baseline. Periodic updating by using the Assessment Tool will provide a basis for monitoring progress. Use and results of the Assessment Tool are for the benefit of the user downloading it. Workflow remains solely with the user and there is no tracking, ranking or reporting back of results. The Assessment Tool can also be found in its online format at: http://www.combattingcybercrime.org/.

Level 1	Level 2	Level 3	Level 4	Response
Non-Legal Framework	National Strategy/Policy?	Binding all relevant authorities and Private Sectors?	Binding Public & Private	○ Yes ○ No
			Binding Public	○ Yes ○ No
			No binding Force	○ Yes ○ No
		Long term strategy?	Longer than 5 years	○ Longer than 5 years
			Longer than 3 years	○ Longer than 3 years
			Less than 3 years	○ Less than 3 years
			No specific terms	○ No specific terms
		Define specific Vulnerable Areas to be protected?		○ Yes ○ No
		Define Resources and Necessities to fight Cybercrime	HR	○ Yes ○ No
			Assets incl. devices & Infra	○ Yes ○ No
		User Protection Strategy		○ Yes ○ No
		Update plan?		○ Yes ○ No
	Lead Government Institution responsible for coordinating the prevention and combating cybercrime	higher than PM		○ Yes ○ No
		Ministerial level		○ Yes ○ No
		lower than Ministerial		○ Yes ○ No

View citations at the end of this section page 406

Synthetic In-Country Assessment Tool (Assessment Table)

Continued from last page

Level 1	Level 2	Level 3	Level 4	Response
Non-Legal Framework	Public-Private Partnership to obtain information and/or evidence?	Formal Cooperation with Private Sector	By Court Order	○ Yes ○ No
			by Prosecutor's Order	○ Yes ○ No
			by Police Letter	○ Yes ○ No
		Informal Cooperation with Private Sector		○ Yes ○ No
	Maintain Statistical Information?	Designated authority to collect & analyze statistics?		○ Yes ○ No
		Define statistics necessary for cybercrime?		○ Yes ○ No
		Updates regularly?		○ Yes ○ No
	Technical Cooperation?			○ Yes ○ No

View citations at the end of this section page 406

E
APPENDIX
TABLE E

Synthetic In-Country Assessment Tool (Assessment Table)

Level 1	Level 2	Level 3	Level 4	Response
Legal Framework	Domestic Legislation on cybercrime?	Cybercrime is regulated by law?	Comprehensively Yes	○ Comprehensively Yes ○ Partially/Draft ○ Partially/No-Draft ○ No, but Draft ○ No
			Partially /Draft	
			Partially /No-Draft	
			No but Draft	
		Have detailed definition related to cybercrime?		○ Yes ○ No
	Joined any Treaties?	signed		○ Yes ○ No
		ratified		○ Yes ○ No

View citations at the end of this section page 406

Synthetic In-Country Assessment Tool (Assessment Table)

Level 1	Level 2	Level 3	Level 4	Response
Substantive Law	Criminalization of traditional crime committed by/through computer related activities			○ Yes ○ No
	Criminalization of newly emerged cybercrime			○ Yes ○ No
	Criminal liability of corporate entity			○ Yes ○ No
	aid, abet and attempt	Aid or Abet		○ Yes ○ No
		Attempt		

View citations at the end of this section page 406

E
APPENDIX
TABLE E

Synthetic In-Country Assessment Tool (Assessment Table)

Level 1	Level 2	Level 3	Level 4	Response
Procedural Law	Due Process	Conditions and Safeguards	During Investigation	○ Yes ○ No
			During Prosecution	○ Yes ○ No
	Investigation	Production order through interception of content data	Production order: Specified computer data	○ Yes ○ No
			Production order: Subscriber information	○ Yes ○ No
		Search and Seizure of computer data and/or computer systems		○ Yes ○ No
		Real-time collection of traffic data		○ Yes ○ No
		Interception of Content Data		○ Yes ○ No
		Trans-border access to computer data		○ Yes ○ No
		Obtaining evidence from 3rd parties	Compelling third parties	○ Yes ○ No
			Compelling service providers to provide information	○ Yes ○ No
	Prosecution	Preservation of stored data		○ Yes ○ No
		Preservation of traffic data		○ Yes ○ No
		Preservation of computers or storage media		○ Yes ○ No

View citations at the end of this section page 406

E
APPENDIX
TABLE E

Synthetic In-Country Assessment Tool (Assessment Table)

Level 1	Level 2	Level 3	Level 4	Response
E-evidence	Rules specific to e-evidence	Rules on admissibility of electronic evidence		○ Yes ○ No
		Rules on admissibility of electronic evidence obtained abroad		○ Yes ○ No
		Rules on discovery of electronic evidence		○ Yes ○ No
		Rules on evaluating probative value of electronic evidence		○ Yes ○ No
		Other rules specific to electronic evidence		○ Yes ○ No
		Evidentiary law specific to cybercrime		○ Yes ○ No
	Law enforcement and e-Evidence	Collecting E-evidence with integrity		○ Yes ○ No
		Storing/retaining e-evidence		○ Yes ○ No
		Transferring e-evidence to courts or prosecutors from Law enforcement agencies		○ Yes ○ No
		Obtaining e-evidence from foreign jurisdiction	Formal MLA	○ Yes ○ No
			Informal MLA	○ Yes ○ No
			Direct Contact with service provider	○ Yes ○ No
			24/7 network	○ Yes ○ No

View citations at the end of this section page 406

E
APPENDIX
TABLE E

Synthetic In-Country Assessment Tool (Assessment Table)

Level 1	Level 2	Level 3	Level 4	Response
Jurisdiction	Common national basis of Jurisdiction	Territory basis	Offence is committed (partly or wholly) within its territory (Territorial principle)	○ Yes ○ No
			Offence is committed using computer system/data located within its territory	○ Yes ○ No
			Offence is directed against computer system/data within its territory	○ Yes ○ No
			Effects/damages of the offence are located within its territory	○ Yes ○ No
			Offence is committed on Ships/Aircrafts	○ Yes ○ No
		Nationality basis	offender's nationality	○ Yes ○ No
			victim's nationality	○ Yes ○ No
	Jurisdiction where extradition is refused			○ Yes ○ No
	Concurrent Jurisdiction			○ Yes ○ No
	Establishment of the place where offences occurred			○ Yes ○ No
	Dual criminality			○ Yes ○ No
	Reservation			○ Yes ○ No

View citations at the end of this section page 406

Synthetic In-Country Assessment Tool (Assessment Table)

Level 1	Level 2	Level 3	Level 4	Response
Safeguards	Data Protection	Limit on the collection of data		○ Yes ○ No
		Purpose of collected data specified at time of collection		○ Yes ○ No
		Use of the data specified		○ Yes ○ No
		Reasonable data security in place		○ Yes ○ No
		Individual has the right to know if government has information about him/her		○ Yes ○ No
		Is the personal data relevant, necessary, accurate and complete?		○ Yes ○ No
		Right to seek redress		○ Yes ○ No
	The right of communication	Freedom of expression expressed in the law		○ Yes ○ No
		the right to information expressed in the law		○ Yes ○ No

View citations at the end of this section page 406

E
APPENDIX
TABLE E

Synthetic In-Country Assessment Tool (Assessment Table)

Level 1	Level 2	Level 3	Level 4	Response
International Cooperation	General	General Principle		○ Yes ○ No
		Extradition	domestic legislation	○ Yes ○ No
			treaties	○ Yes ○ No
			central authority	○ Yes ○ No
			refusal of extradition	○ Yes ○ No
			dual criminality	○ Yes ○ No
			seriousness of a minimum penalty	○ Yes ○ No
	Formal	General principles on Mutual Legal Assistance	domestic legislation for MLA	○ Yes ○ No
			treaties	○ Yes ○ No
			central authority	○ Yes ○ No
			expedited means of MLA	○ Yes ○ No
			refusal of MLA request	○ Yes ○ No
			dual criminality	○ Yes ○ No
			confidentiality of information to be provided and limitation on use	○ Yes ○ No
			spontaneous information	○ Yes ○ No
		Specific Provisions on Mutual Legal Assistance	provisional measures	○ Yes ○ No
			investigative powers	○ Yes ○ No
	Informal		Multi-lateral Networks (e.g., 24/7)	○ Yes ○ No
			Bilateral Coop Network	○ Yes ○ No

View citations at the end of this section page 406

E
APPENDIX
TABLE E

Synthetic In-Country Assessment Tool (Assessment Table)

Level 1	Level 2	Level 3	Level 4	Response
Capacity Building	CERT			○ Yes ○ No
	Law Enforcement	Law enforcement structure for cybercrime cases		○ Yes ○ No
		Separate unit/agency specifically for investigating cybercrime cases		○ Yes ○ No
		Specialized law enforcement officers assigned to cybercrime cases		○ Yes ○ No
		Sufficient resources and capabilities to investigate cybercrime cases and/or cases involving electronic evidence (including digital forensic tools)		○ Yes ○ No
		Training programs to police officers for the investigation of cybercrime cases		○ Yes ○ No
	Prosecution	Prosecution structure for cybercrime cases		○ Yes ○ No
		Separate unit/agency specifically for prosecuting cybercrime cases		○ Yes ○ No
		Specialized prosecutors assigned to cybercrime cases		○ Yes ○ No
		Sufficient resources and capacities to prosecute cybercrime cases and/or cases involving e-evidence		○ Yes ○ No
		Training programs to prosecutors for cybercrime cases		○ Yes ○ No
	Court	Court structure for cybercrime cases		○ Yes ○ No
		Separate courts specifically for the trial of cybercrime cases		○ Yes ○ No
		Specialized judges assigned to cybercrime cases		○ Yes ○ No
		Training programs to judges for the trial of cybercrime cases		○ Yes ○ No

View citations at the end of this section page 406

End Notes

Referenced in: Appendix B

1. African Union. 2014 (Adopted on 27 Jun. 2014). African Union Convention on Cyber Security and Personal Data Protection.
2. Commonwealth of Independent States (CIS). 2001(Done on 1 Jun. 2001). Agreement on cooperation among the States members of the Commonwealth of Independent States in Combating Offences related to Computer Information.
3. Council of Europe. 2001 (Opened for Signature 23 Nov. 2001). Convention on Cybercrime.
4. League of Arab States. 2010 (Done on 21 Dec. 2010). Arab Convention on Combating Information Technology Offences.
5. Shanghai Cooperation Organization (SCO). 2009 (Done on 16 Jun. 2009). Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security.
6. Economic Community of West African States (ECOWAS). 2011 (Done on 19 Aug. 2011). Directive on Fighting Cybercrime within Economic Community of West African States.
7. Council of Europe. 2003 (Opened for signature on 28 Jan. 2003). Additional Protocol to Convention on Cybercrime Concerning the Criminalization of Acts of a Racist and Xenophobic Nature Committed through Computer Systems.
8. Council of Europe. 2007(Opened for signature on 25 Oct. 2007). Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse.
9. Common Market for Eastern and Southern Africa (COMESA). 2011. "Cybercrime Model Bill, 2011." In 2011 Gazette Volume 16, 45-77. Lusaka: COMESA.
10. Commonwealth Secretariat. 2002. "Annex B – Computer and Computer Related Crimes Bill." In *Model Law on Computer and Computer Related Crime*, 15-24. London: The Commonwealth.
11. ITU. 2012. HIPCAR, "Section II: Model Legislative Text – Cybercrime/e-Crimes." *Cybercrime/e-Crimes: Model Policy Guidelines & Legislative Texts*, 15-28. Geneva: ITU.
12. ITU. 2013. HIPSSA, *Computer Crime and Cybercrime: Southern African Development Community (SADC) Model Law.* Geneva: ITU.
13. ITU. 2013. ICBRPAC, *Electronic Crimes: Knowledge-Based Report (Skeleton).* Geneva: ITU.
14. ITU. 2013. HIPCAR, "Section II: Model Legislative Text –Electronic Crimes." *Electronic Evidence: Model Policy Guidelines and Legislative Texts*, 13-20. Geneva: ITU.
15. Organization for Eastern Caribbean States (OECS). 2011. Electronic Crimes Bill (Fourth Draft). Castries: OECS.

Referenced in: Appendix C

1. Unless otherwise noted, information contained in this Appendix was verified as of 16 June 2016.

2. 196 countries are included in this list. Countries are included if they are either (1) a Member of the World Bank ("Member Countries: International Bank for Reconstruction and Development"; http://www.worldbank.org/en/about/leadership/members (last visited 4 February 2016), (2) a Member State of the UN ("Member States of the United Nations"; http://www.un.org/en/member-states/ (last visited 4 February 2016)); or (3) Permanent Observers to the UN ("Permanent Observers: Non-member States"; http://www.un.org/en/sections/member-states/non-member-states/index.html (last visited 4 February 2016).

3. The instruments cited here are discussed in more detail in subchapter 5 A. Membership of a country in an international or regional instrument is indicated as follows: Blue =Yes, has signed and/or ratified (or acceded to) the instrument; Light Blue = has been invited to accede to the instrument; No color = No membership. The Africa Union Convention (https://www.au.int/web/en/treaties/african-union-convention-cyber-security-and-personal-data-protection) (last accessed 30 August 2016) is not dealt with here because of the 54 potential members to the Convention only 8 have signed it and none have ratified it.

Referenced in: Appendix D

1. **The AIDP Assessment is based on a number of background papers prepared by its members. Among these are:**

   - Weigend, Thomas. 2012. "Section 1: Concept paper and questionnaire." Paper prepared for AIDP's Preparatory Colloquium Section I for the 19th International Congress of Penal Law on Information Society and Penal Law, "Criminal Law General Part," Verona, Italy, 28-30 November.

   - Nijboer, Johannes F. 2013. "Section 3: Concept Paper and Questionnaire." Paper prepared for AIDP's Preparatory Colloquium Section III for the 19th International Congress of Penal Law on Information Society and Penal Law, "Criminal Procedure," Antalya, Turkey, 23-26 September.

   - Klip, André. 2013. "Section 4: Concept Paper and Questionnaire." Paper prepared for AIDP's Preparatory Colloquium Section IV for the 19th International Congress of Penal Law on Information Society and Penal Law, "International Criminal Law," Helsinki, Finland, 10-12 June.

   - Viano, Emilio, *"Section 2: Concept Paper and Questionnaire."* Paper presented at the Preparatory Colloquium: Section II (Criminal Law, Special Part) for the 20th International Congress of Penal Law on "Information Society and Penal Law", 2013, AIDP, at 1 to 5, at: http://www.penal.org/IMG/pdf/Section_II_EN.pdf.

2. Country Profile (*Questionnaire in preparation of the Conference*), 2007, Council of Europe. (Paper prepared for the Octopus Interface Conference, "Conference on Cooperation against Cybercrime," Strasbourg, 11-12 June, 2007), at: http://www.coe.int/t/dghl/cooperation/economiccrime/Source/567-m-if%202008%20quest_en.doc. This questionnaire refers to provisions in national legislation corresponding to the provisions of the Budapest Convention. Additional resources - country profiles and numerous questionnaires to parties and observers - are available at: http://www.coe.int/en/web/cybercrime/country-profiles and http://www.coe.int/en/web/cybercrime/t-cy-reports.

3. *Toolkit for Cybercrime Legislation (Draft), Country Worksheet,* 2010, ITU, at 39 to 50 (ITU Country Worksheet), at: http://www.cyberdialogue.ca/wp-content/uploads/2011/03/ITU-Toolkit-for-Cybercrime-Legislation.pdf.

4. *ICB4PAC, Electronic Crimes: Knowledge-Based Report (Assessment), Annex 1: Questionnaire,* 2013, ITU, at 123 to 124, at: http://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/ICB4PAC/Documents/FINAL%20DOCUMENTS/cybercrime_assessment.pdf.

5. *Cybercrime Questionnaire for Member States,* 2012, UNODC, at: https://cms.unov.org/DocumentRepositoryIndexer/GetDocInOriginalFormat.drsx?DocID=f4b2f468-ce8b-41e9-935f-96b1f14f7bbc.

6. University of Oxford, Global Cyber Security Capacity Centre. 2014. "Dimension 4 –Legal and regulatory frameworks, D4-1: Cyber security legal frameworks and D4-2: Legal Investigations." In *Cyber Security Capability Maturity Model (CMM) – Pilot,* 26-32. University of Oxford, Global Cyber Security Capacity Centre.

7. "Media" – as used here means any device capable of storing digital or electronic data, such as, but not limited to, computer hard drives, memory card, disk, or USB-device, for example.

Referenced in: Appendix E

1. This would include, for example, definitions of "computer system", "computer data", "service provider", "subscriber information" and "traffic data".
2. "Ratified" as used in this Assessment Table would also include "acceded to".
3. These would include: Illegal access to a computer system; Illegal Interception; Data Interference; System Interference; and Misuse of Devices as well as Computer-related fraud; Computer-related forgery; Computer-related copyright and trademark offences; Computer-related identity offences.
4. Such issues would include: financial crimes; sending SPAM; and computer-related child pornography offences.
5. E.g. reciprocity through a treaty of comity
6. Due process issues refer to the rights of the accused during investigations and at trial. What constitutes "due process" varies from country to country and legal system. These could include, without limitation, the right not to testify, the right to a fair trial, the right to confront one's accuser, the right to counsel, etc. Accordingly, rather than enumerate specific rights, the Assessment seeks to record whether any such rights exist at the investigatory and prosecutorial levels.
7. This refers to legislation on extradition, as opposed to cybercrime.
8. Treaty here refers to an "extradition" treaty, as opposed to a cybercriome treaty.

Bibliography

In this Chapter

Bibliography

Books, Reports, Journals, Studies, Working Papers, Conference Papers, News Release, Blogs, Online encyclopedia articles and Electronic magazines

Jump to section:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

A

Abramovitch, Daniel Y. and Gene F. Franklin. 2002. "A Brief History of Disk Drive Control." *IEEE Control Systems Magazine* 22(3): 28–42.

Abreu, Elinor Mills. 2001 (Posted on 12 Dec. 2001). "FBI confirms "Magic Lantern" Project Exists." *Reuters*. http://www.uhuh.com/control/magicfbi.htm.

Acunetix. "SQL Injection." *Acunetix*. http://www.acunetix.com/websitesecurity/sql-injection/.

Adler, Julie. 2011. "The Public's Burden in a Digital Age: Pressures on Intermediaries & the Privatization of Internet Censorship." *Journal of Law & Policy* 20(1): 231 –265. http://brooklynworks.brooklaw.edu/cgi/viewcontent.cgi?article=1093&context=jlp.

African Union. 2016. "List of Countries Which Have Signed, Ratified/Acceded to the AU Convention." *African Union*. https://www.au.int/web/sites/default/files/treaties/29560-sl-african_union_convention_on_cyber_security_and_personal_data_protection.pdf.

Agresta, Michael. 2012 (Posted on 17 Aug. 2012). "Will the Next Election Be Hacked?" *Wall Street Journal*. http://www.wsj.com/articles/SB10000872396390444508504577595280674870186

Ahmed, Saeed. 2015 (Posted on 4 Dec. 2015). "Who Were Syed Rizwan Farook and Tashfeen Malik?" *CNN*. http://www.cnn.com/2015/12/03/us/syed-farook-tashfeen-malik-mass-shooting-profile/index.html.

Akers, Ronald L. 1997. *Criminological Theories: Introduction and Evaluation* (2nd Edition). Los Angeles: Roxbury.

Al Jazeera. 2017 (Posted on 16 May 2017)."WannaCry: What Is Ransomware and How to Avoid It." *Al Jazeera*. http://www.aljazeera.com/news/2017/05/ransomware-avoid-170513041345145.html.

Albertson, Mark. 2013 (Posted 6 Dec. 2013). "Singapore Cyberstalker Convicted, but Others Roam Free." *Examiner*. http://www.examiner.com/article/singapore-cyberstalker-convicted-but-others-roam-free.

Amann, Diane Marie, ed. 2014. "Jurisdictional, Preliminary and Procedural Concerns." *Benchbook on International Law:* II.A-1 to 16. https://www.asil.org/sites/default/files/benchbook/jurisdiction.pdf.

American Law Institute. "Model Code of Cybercrime Investigative Procedure." *American Law Institute*. http://www.crime-research.org/library/Model_Code.htm.

Amnesty International. 2016. *Encryption: A Matter of Human Right*. Washington D.C.: Amnesty International. http://www.amnestyusa.org/sites/default/files/encryption_-_a_matter_of_human_rights_-_pol_40-3682-2016.pdf.

Apple. 2016 (Posted on 16 Feb. 2016). "A Message to Our Customers." *Apple*. http://www.apple.com/customer-letter/.

Armstrong, Jonathan, Gayle McFarlane and André Bywater. 2015. "European Court Rules Safe Harbor Invalid in Schrems Case." *Cordery Compliance Limited*. http://www.corderycompliance.com/european-court-rules-safe-harbor-invalid-in-schrems-case/.

Ashford, Warwick. 2014 (Posted on 27 Oct. 2014). "Researchers Uncover Sophisticated Cyber Espionage Campaign." *Computer Weekly*. http://www.computerweekly.com/news/2240233415/Researchers-uncover-sophisticated-cyber-espionage-campaign.

Ashford, Warwick. 2015 (Posted on 2 Mar. 2015). "National Crime Agency Leads Partnership to Guard UK against Cybercrime." *Computer Weekly*. http://www.computerweekly.com/news/2240241511/National-Crime-Agency-leads-partnership-to-guard-UK-against-cyber-crime.

Ashford, Warwick. 2015 (Posted on 5 Jun. 2015). "Co-Operation Driving Progress in Fighting Cyber Crime, Say Law Enforcers." *Computer Weekly*. http://www.computerweekly.com/news/4500247603/Co-operation-driving-progress-in-fighting-cyber-crime-say-law-enforcers.

Ashford, Warwick. 2015 (Posted on 29 Jun. 2015). "Police Arrest 130 In Global Anti-cyber Fraud Operation." *Computer Weekly*. http://www.computerweekly.com/news/4500248925/Police-arrest-130-in-global-anti-cyber-fraud-operation.

APEC (Asia-Pacific Economic Cooperation). 2009. *APEC Cross-border Privacy Enforcement Arrangement*. Singapore: APEC. http://www.apec.org/~/media/Files/Groups/ECSG/CBPR/CBPR-CrossBorderPrivacyEnforcement.pdf.

Ausloos, Jef. 2012. "The Right to Be Forgotten—Worth Remembering?" *Computer Law and Security Review* 28 (1): 143–52.

Australian Government, Attorney-General's Department. 2015. *Data Retention: Guidelines for Service Providers.* Barton ACT 2600, Australia: Australian Government, Attorney-General's Department. https://www.ag.gov.au/NationalSecurity/DataRetention/Documents/DataRetentionGuidelinesForServiceProviders.pdf.

Australian Government, Attorney-General's Department. 2015. *Discussion Paper--Mandatory Data Breach Notification.* Barton ACT 2600, Australia: Australian Government, Attorney-General's Department. https://www.ag.gov.au/Consultations/Documents/data-breach-notification/Consultation-draft-data-breach-notification-2015-discussion-paper.DOCX.

Avina, Jeffrey. 2011. "Public-private Partnerships in the Fight against Crime." *Journal of Financial Crime* 18(3): 282 –291. http://www.emeraldinsight.com/doi/pdfplus/10.1108/13590791111147505.

B

Bacon, Stephen L. 2011. "A Distinction without a Difference: "Receipt" and "Possession" of Child Pornography and the Double Jeopardy Problem." *University of Miami Law* Review 65(3): 1027 –1058. http://lawreview.law.miami.edu/wp-content/uploads/2011/12/v65_i3_sbacon.pdf.

Bajaj, Avneet Kaur and Chander Jyoti.2015. "Cyber Crime through Mobile Phone in India and Preventive Methods." *International Journal of Research & Review* 2(3): 110 – 113. http://www.gkpublication.in/IJRR_Vol.2_Issue3_March2015/IJRR0033.pdf.

Bajarin, Tim. 2014 (Posted on 13 Jan. 2014). "The Next Big Thing for Tech: The Internet of Everything." *Time*. http://time.com/539/the-next-big-thing-for-tech-the-internet-of-everything/.

Bambauer, Derek. 2013. "Privacy Versus Security." *Journal of Criminal Law & Criminology* 103(3). http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=7454&context=jclc.

Banisar, David & Gus Hosein. 2000. *A Draft Commentary on the Council of Europe Cybercrime Convention.* Privacy Lecture Series. http://privacy.openflows.org/pdf/coe_analysis.pdf.

Baranjuk, Chris. 2015 (Posted on 30 Oct. 2015). "Tor Launches Anti-Censorship Messenger Service." *BBC News*. http://www.bbc.com/news/technology-34677323.

Baraniuk, Chris. 2017 (Posted on 20 Jul. 2017). "AlphaBay and Hansa Dark Web Markets Shut Down." *BBC News*. http://www.bbc.com/news/technology-40670010.

Barendt, Eric. 2012. "Freedom of Speech and Privacy." *Free Speech Debate*. http://freespeechdebate.com/en/discuss/freedom-of-speech-and-privacy/.

Barrett, David. 2013 (Posted on 10 Jul. 2013). "One Surveillance Camera for Every 11 People in Britain, Says CCTV Survey." *Telegraph*. http://www.telegraph.co.uk/technology/10172298/One-surveillance-camera-for-every-11-people-in-Britain-says-CCTV-survey.html.

Bauer, Johannes M. & William H. Dutton. 2015. "The New Cybersecurity Agenda: Economic and Social Challenges to a Secure Internet." Background Paper for the World Development Report (WDR) 2016. Washington D.C.: World Bank. https://openknowledge.worldbank.org/handle/10986/23641.

Baum, Katrina, Shannan Catalano, Michael Rand & Kristina Rose. 2009. "Stalking Victimization in the United States." U.S. Department of Justice, Office of Justice Programs. https://www.justice.gov/sites/default/files/ovw/legacy/2012/08/15/bjs-stalking-rpt.pdf.

Baylon, Caroline, Roger Brunt and David Livingstone. 2015. *Cyber Security at Civil Nuclear Facilities Understanding the Risks*. London: The Royal Institute of International Affairs, Chatham House. https://www.chathamhouse.org/sites/files/chathamhouse/field/field_document/20151005CyberSecurityNuclearBaylonBruntLivingstone.pdf.

Beal, Vangie. "Big Data." *Webopedia*. http://www.webopedia.com/TERM/B/big_data.html.

Bearman, Joshua & Tomer Hanuak. 2015 (Posted on May 2015). "The Rise & Fall of Silk Road." *Wired*. https://www.wired.com/2015/04/silk-road-1/.

Becker, Jay. 1980. "The Trial of a Computer Crime." *Computer Law Journal* 2. http://repository.jmls.edu/cgi/viewcontent.cgi?article=1610&context=jitpl.

Berkman Center for Internet & Society. "State and Federal Stalking Laws." *Harvard University*. https://cyber.law.harvard.edu/vaw00/cyberstalking_laws.html.

Bernstein, Anita. 2012. "Real Remedies for Virtual Injuries." *North Carolina Law Review* 90: 1457–1490. http://brooklynworks.brooklaw.edu/cgi/viewcontent.cgi?article=1447&context=faculty.

Bheemaiah, Kariappa. 2015 (Posted on Jan. 2015). "Block Chain 2.0: The Renaissance of Money." *Wired*. https://www.wired.com/insights/2015/01/block-chain-2-0/.

Bilge, Leyla, Thorsten Strufe, Davide Balzaroti & Engin Kirda. 2009. "All Your Contacts Belong to Us: Automated Identity Theft Attacks on Social Networks." Paper prepared for the 18th international conference on World Wide Web, Madrid, 20-24 Apr. http://seclab.tuwien.ac.at/papers/www-socialnets.pdf.

BI Intelligence. 2016 (Posted on 25 May 2016). "Samsung Is Building a Smart Cities Network in South Korea." *BI Intelligence*. http://www.businessinsider.com/samsung-is-building-a-smart-cities-network-in-south-korea-2016-5.

Bisson, David. 2014 (Posted on 23 Mar. 2014). "5 Social Engineering Attacks to Watch Out for." *Tripwire*. https://www.tripwire.com/state-of-security/security-awareness/5-social-engineering-attacks-to-watch-out-for/.

Blagov, Sergei. 2015. (Posted on 2 Sep. 2015). "Multinationals to Meet Russia Data Localization Rules." *Bloomberg BNA: News*. http://www.bna.com/multinationals-meet-russia-n17179935650/.

Blagov, Sergei. 2015 (Posted on Aug. 5 2015). "Russia Clarifies Looming Data Localization Law." *Bloomberg BNA: News*. http://www.bna.com/russia-clarifies-looming-n17179934521/.

Blake, Andrew. 2016 (Posted on 7 Oct. 2016). "Attorney for Silk Road Mastermind Ross Ulbricht Challenges Conviction in Federal Appeals Court." *Washington Times*. http://www.washingtontimes.com/news/2016/oct/7/appeals-court-hears-case-against-ross-ulbricht-con/.

Blau, John. 2007 (5 Sep. 2007). "Debate Rages over German Government Spyware Plan." *InfoWorld*. http://www.infoworld.com/article/2649377/security/debate-rages-over-german-government-spyware-plan.html.

Blumenthal, Jeremy A. 2001. "Shedding Some Light on Calls for Hearsay Reform: Civil Law Hearsay Rules in Historical and Modern Perspective." *Pace International Law Review* 13, no.1. http://digitalcommons.pace.edu/cgi/viewcontent.cgi?article=1205&context=pilr.

Borchers, Detlef. 2007. (Posted on 19 Jul. 2007). "Secret Online Search Warrant: FBI uses CIPAV for the first time." *Heise News*. http://www.h-online.com/security/news/item/Secret-online-search-warrant-FBI-uses-CIPAV-for-the-first-time-733274.html.

Borisevich, Galina, Natalya Chernyadyeva, Evelina Frolovich, Pavel Pastukhov, Svetlana Polyakova, Olga Dobrovlyanina, Deborah Griffith Keeling and Michael M. Losavio. 2012. "A Comparative Review of Cybercrime Law and Digital Forensics in Russia, the United States and under the Convention on Cybercrime of the Council of Europe." *Northern Kentucky Law Review* 39(2): 267.

Boué, Thomas. 2015 (Jun. 2015) "Closing the Gaps in EU Cyber Security." *Computer Weekly*. http://www.computerweekly.com/opinion/Closing-the-gaps-in-EU-cyber-security.

Bourke, Latika. 2016. "WhatsApp Gets Full Encryption to Protect User Privacy." *The Sydney Morning Herald,* April 6. http://www.smh.com.au/technology/smartphone-apps/whatsapp-gets-full-encryption-to-protect-user-privacy-20160405-gnzaf2.html#ixzz453LPLDus.

Brenner, Susan W. 2001. "Cybercrime Investigation and Prosecution: the Role of Penal and Procedural Law." *Murdoch University Electronic Journal of Law* 8(2). http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN003073.pdf.

Brenner, Susan W. and Bert-Jaap Koops. 2004. "Approaches to Cybercrime Jurisdiction." *Journal of High Technology Law* 4(1): 1-46. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=786507.

Brenner, Susan W. 2007. "Cybercrime: Re-thinking Crime Control Strategies." In Crime *Online* edited by Yvonne Jewkes, 12–28. Cullompton: Willan Publishing.

Brenner. Susan W. 2007. "Private-public Sector Cooperation in Combating Cybercrime: in Search of a Model." *Journal of International Law and Technology* 2(2): 58 –67. http://www.jiclt.com/index.php/jiclt/article/view/20.

Brenner, Susan W. 2009 (Posted on 6 May 2009). "Thoughts, Witches and Crimes." *CYB3RCRIM3: Observations on Technology, Law, and Lawlessness*. http://cyb3rcrim3.blogspot.com/2009/05/thoughts-witches-and-crimes.html.

Brenner, Susan W. 2010 (Posted on 7 Jun. 2010). "Time Period for Seizing Computers." *CYB3RCRIM3: Observations on Technology, Law, and Lawlessness*. http://cyb3rcrim3.blogspot.com/2009/05/thoughts-witches-and-crimes.html.

Brezinski, D. and Tom Killalea. 2002. *Guidelines for evidence collection and archiving.* IETF RFC 3227.

BBA (British Bankers' Association). 2014. The cyber Threat to Banking: *A Global Industry Challenge.* London: BBA. https://www.bba.org.uk/wp-content/uploads/2014/06/BBAJ2110_Cyber_report_May_2014_WEB.pdf.

BBC (British Broadcasting Corporation). 2010. (Posted on 9 Dec. 2010). "Anonymous Hacktivists Say Wikileaks War to Continue." *BBC*. http://www.bbc.com/news/technology-11935539.

BBC Monitoring Europe. 2015 (Posted on 23 Mar. 2015). "New Bill Gives Turkish Government Power to Shut Down Websites in Four Hours." *BBC*.

BBC News. 2014 (Posted on17 Jan. 2014). "Edward Snowden: Leaks that Exposed US Spy Programme." *BBC News*. http://www.bbc.com/news/world-us-canada-23123964.

BBC News. 2016 (Posted on 22 Jul. 2016). "Snowden Designs Phone Case to Spot Hack Attacks." *BBC News*. http://www.bbc.com/news/technology-36865209.

BBC News. 2017 (Posted on 14 Feb. 2017). "How Hackers Could Use Doll to Open Your Front Door." *BBC News*. http://www.bbc.com/news/technology-38966285.

BBC News. 2017 (Posted on 14 May 2017). "Ransomware Cyber-attack Threat Escalating—Europe." *BBC News*. http://www.bbc.com/news/technology-39913630.

BBC News. 2017 (Posted on 14 May 2017). "Next Cyber-attack Could Be Imminent, Warn Experts." *BBC News*. http://www.strategic-culture.org/news/2017/05/14/international-cyber-attack-roots-traced-us-national-security-agency.html.

BBC News. 2017 (Posted on 23 May 2017). "More Evidence for WannaCry 'Link' to North Korean Hackers." *BBC News*. http://www.bbc.com/news/technology-40010996.

Broache, Anne. 2007 (Posted on 31 Aug. 2007). "Germany Wants to Sic Spyware on Terror Suspects." *CNET*. http://www.cnet.com/news/germany-wants-to-sic-spyware-on-terror-suspects/.

Brown, Cameron S.D. 2015. "Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice." *International Journal of Cyber Criminology* 9(1): 55-119. http://www.cybercrimejournal.com/Brown2015vol9issue1.pdf.

Brown, Christopher L. T. 2006. *Computer Evidence: Collection and Preservation* (1st Edition). Newton Centre: Charles River Media.

Bucci, Steven, Paul Rosenzweig & David Inserra. "A Congressional Guide: Seven Steps to US Security, Prosperity, and Freedom in Cyberspace." *Heritage Foundation*. http://www.heritage.org/research/reports/2013/04/a-congressional-guide-seven-steps-to-us-security-prosperity-and-freedom-in-cyberspace.

Budd, Christopher. 2014 (Posted on 3 Feb. 2014). "Why the SpyEye Conviction is a Big Deal." *Trend Micro*. http://blog.trendmicro.com/spyeye-conviction-big-deal/.

Burns, Brett. 2012. "Level 85 Rogue: When virtual Theft Merits Criminal Penalties." *UMKC Law Review* 80(3): 831.

BSA (Business Software Alliance). 2015. *EU Cybersecurity Dashboard: A Path to a Secure European Cyberspace*. Washington D.C.: BSA. http://www.bsa.org/~/media/Files/Policy/Security/EU/study_eucybersecurity_en.pdf.

Buttarelli, Giovanni. 2011. "Security and Civil Liberties in the Fight against Cybercrime: Fundamental Legal Principles for a Balanced Approach." Courmayeur: ISPAC (International Scientific and Professional Advisory Council of the United Nations Crime Prevention and Criminal Justice Programme). https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Speeches/2011/11-12-02_Cybercrime_speech_GB_EN.pdf.

C

Calabresi, Massimo. 2017 (Posted on 22 Jun. 2017). "Election Hackers Altered Voter Rolls, Stole Private Data, Officials Say." *Time*. http://time.com/4828306/russian-hacking-election-widespread-private-data/.

California Department of Justice, Office of the Attorney General. 2014. *California Data Breach Report*. California Department of Justice, Office of the Attorney General. https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/2014data_breach_rpt.pdf.

Callanan, Cormac and Gercke, Marco. 2008. *Cooperation between Law Enforcement and Internet Service Providers against Cybercrime: Towards Common Guidelines Best-of-Breed Guidelines.* Strasburg: Council of Europe. http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Documents/Reports-Presentations/567%20prov-d-wg%20STUDY%20final%20_25%20june%202008_.pdf.

Caloyannides, Michael A. 2004. *Privacy Protection and Computer Forensics* (2nd Edition). Norwood: Artech House. http://www.pdfarchive.info/pdf/C/Ca/Caloyannides_Michael_A_-_Privacy_protection_and_computer_forensics.pdf.

Cannataci, Joseph A. & Mireille M. Caruana. 2014. *Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (T-PD).* Strasbourg: CoE. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806ae16a.

Carlisle, David. 2017. "Virtual Currencies and Financial Crimes." RUSI Occasional Paper, Royal United Services Institute for Defence and Security Studies (RUSI). https://rusi.org/sites/default/files/rusi_op_virtual_currencies_and_financial_crime.pdf.

Carlson, Eric and Livingston, Scott. 2014 (Posted on 12 Aug. 2014). "Fraud Investigators Imprisoned for Illegally Collecting Personal Data in China." *Convington & Burling LLP –Inside Privacy.* https://www.insideprivacy.com/international/fraud-investigators-imprisoned-for-illegally-collecting-personal-data-in-china/.

Carney, Megan and Marc Rogers. 2004. "The Trojan Made Me Do It: A First Step in Statistical Based Computer Forensics Event Reconstruction." *International Journal of Digital Evidence* 2(4). https://www.utica.edu/academic/institutes/ecii/publications/articles/A0B2CCCB-E6FC-6840-AF4A01356B9B687A.pdf.

Casey, Eoghan. 2000. *Digital Evidence and Computer Crime: Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet* (1st Edition). London: Academic Press.

Casey, Eoghan. 2002. "Error, Uncertainty and Loss in Digital Evidence." *International Journal of Digital Evidence* 1(2). https://www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

Casey, Eoghan. 2002. "Practical Approaches to Recovering Encrypted Digital Evidence." *International Journal of Digital Evidence* 1(3). https://www.utica.edu/academic/institutes/ecii/publications/articles/A04AF2FB-BD97-C28C-7F9F4349043FD3A9.pdf.

Casey, Eoghan. 2004. *Digital Evidence and Computer Crime: Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet* (2d ed.). London: Academic Press.

Cassin, Richard L. 2015 (Posted on 11 Sep. 2015). "A Different World after 9/11: Egmont Group Statement on Global Fight against Terrorist Financing." *The FCPA Blog*. http://www.fcpablog.com/blog/2015/9/11/a-different-world-after-911-egmont-group-statement-on-global.html.

Castells, Manuel. 2002. *The Internet Galaxy: Reflections on the Internet, Business, and Society.* Oxford: Oxford University Press.

Cate, Fred H., Peter Cullen and Viktor Mayer-Schönberger. 2014. *Data Protection Principles for the 21st Century Revising the 1980 OECD Guideline.* Oxford: Oxford Internet Institute, University of Oxford. http://www.oii.ox.ac.uk/publications/Data_Protection_Principles_for_the_21st_Century.pdf.

Catteddu, Daniele and Giles Hogben, eds. 2009. *Cloud Computing: Benefits, Risks and recommendations for Information Security.* Heraklion: ENISA (European Network and Information Security Agency). https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment/at_download/fullReport.

Cecil, Nicholas. 2011 (Posted on 6 Nov. 2011). "MP Demands Law to Force Internet Providers to Remove Gang Videos." *Evening Standard*. http://www.standard.co.uk/news/mp-demands-law-to-force-internet-providers-to-remove-gang-videos-6365780.html.

CDT (Center for Democracy & Technology). 2012. *Shielding the Messengers: Protecting Platforms for Expression and Innovation* (Version 2, Updated December 2012). Washington, D.C.: CDT. https://cdt.org/files/pdfs/CDT-Intermediary-Liability-2012.pdf.

CSIS (Center for Strategic and International Studies). 2014. *Net Losses: Estimating the Global Cost of Cybercrime (Economic impact of cybercrime II).* Washington D.C.: CSIS. http://csis.org/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf.

Chandran, Nyshka. 2016 (Posted on 25 Jan. 2016). "Facebook's Troubles in India Keep Snowballing." *CNBC*. http://www.cnbc.com/2016/01/25/facebook-struggles-to-lift-ban-on-free-basics-in-india.html.

Chang, Weiping, Wingyan Chung, Hsinchun Chen and Shihchieh Chou. 2003. "An International Perspective on Fighting Cybercrime." In: *Intelligence and Security Informatics: First NSF/NIJ Symposium, ISI 2003, Tucson, AZ, USA, June 2–3, 2003 Proceedings*, 379-384. Berlin-Heidelberg: Springer.

Chappell, Bill. 2017 (Posted on 15 May 2017). "WannaCry Ransomware: Microsoft Calls Out NSA for 'Stockpiling' Vulnerabilities." *NPR*. http://www.npr.org/sections/thetwo-way/2017/05/15/528439968/wannacry-ransomware-microsoft-calls-out-nsa-for-stockpiling-vulnerabilities.

Chappell, Chappell. 2017 (Posted on 15 May 2017). "WannaCry Ransomware: What We Know Monday." *NPR*. http://www.npr.org/sections/thetwo-way/2017/05/15/528451534/wannacry-ransomware-what-we-know-monday.

Chaski, Carole E. 2005. "Who's at the Keyboard? Authorship Attribution in Digital Evidence Investigations." *International Journal of Digital Evidence* 4(1). https://www.utica.edu/academic/institutes/ecii/publications/articles/B49F9C4A-0362-765C-6A235CB8ABDFACFF.pdf.

Chawki, Mohamed, Ashraf Mohammad Darwish, Ayoub Khan and Sapna Tyagi. 2015. *Cybercrime, Digital Forensics and Jurisdiction.* Berlin: Springer International Publishing.

Cheh, Mary M. 1991. "Constitutional Limits on Using Civil Remedies to Achieve Criminal Law Objectives: Understanding and Transcending the Criminal-Civil Law Distinction." *Hastings Law Journal* 42.

Chein, Allen. 2012. "A Practical Look at Virtual Property." *St. John's Law Review* 80(3) 1059-1090. http://scholarship.law.stjohns.edu/cgi/viewcontent.cgi?article=1211&context=lawreview.

Chia, Terry. 2012 (Posted on 20 Aug. 2012). "Confidentiality, Integrity and Availability (CIA): The Three Components of the CIA Triad." *IT Security Community Blog.* http://security.blogoverflow.com/2012/08/confidentiality-integrity-availability-the-three-components-of-the-cia-triad/.

Chief Judge B. Lynn Winmill, David L. Metcalf & Michael E. Band. 2010. "Cybercrime: Issues and Challenges in the United States." *Digital Evidence & Electronic Signature Law Review* 7.

Chin, Josh. 2015 (Posted on 12 Feb. 2015). "China Internet Restrictions Hurting Business, Western Companies Say." *The Wall Street Journal: China Real Time Report.* http://blogs.wsj.com/chinarealtime/2015/02/12/china-internet-restrictions-hurting-business-western-companies-say/.

Choi, Kyung-shick. 2008. *Structural Equation Modeling Assessment of Key Causal Factors in Computer Crime Victimization: A Dissertation Submitted to the School of Graduate Studies and Research.* In: *Partial Fulfillment of the Requirements for the Degree Doctor of Philosophy.* Indiana University of Pennsylvania. http://knowledge.library.iup.edu/cgi/viewcontent.cgi?article=1444&context=etd.

Chun, Hyun Wook & Ja Young Lee. 2014. "Convention on Cybercrime and Due Process of Law: on Preservation and Partial Disclosure of Stored Data." *Korean Criminological Review* 25 (ii).

Ciardhuain, Séamus Ó. 2004. "An Extended Model of Cybercrime Investigation." *International Journal of Digital Evidence* 3(1). https://www.utica.edu/academic/institutes/ecii/publications/articles/A0B70121-FD6C-3DBA-0EA5C3E93CC575FA.pdf.

Clancy, Thomas K. 2011. *Cyber Crime and Digital Evidence: Materials and Cases.* New York: Lexisnexis.

Clark, Kelli. 2015 (Posted on 27 Oct. 2015). "The EU Safe Harbor Agreement Is Dead, Here's What to Do about It." *Forbes.* http://www.forbes.com/sites/riskmap/2015/10/27/the-eu-safe-harbor-agreement-is-dead-heres-what-to-do-about-it/#2f3bd6757171.

Clay, Jon. 2015 (Posted on 13 Apr. 2015). "Operation SIMDA: The Power of Public/Private Partnerships." *Trend Micro/Simply Security*. http://blog.trendmicro.com/operation-simda-the-power-of-publicprivate-partnerships/.

Clinton, Larry. "Cross cutting Issue #2 How Can We Create Public Private Partnerships that Extend to Action Plans that Work? (Updated)." ISA (Internet Security Alliance). https://www.whitehouse.gov/files/documents/cyber/ISA%20-%20Hathaway%20public%20private%20partnerships.pdf.

Clough, Jonathan. 2011. "Data Theft? Cybercrime and the Increasing Criminalization of Access to Data." *Criminal Law Forum* 22 (1 –2):145–170.

Cohen, Lawrence E. and Marcus Felson. 1979. "Social Change and Crime Rate Trends: A Routine Activity Approach." *American Sociological Review* 44: 588-608. http://www.personal.psu.edu/exs44/597b-Comm%26Crime/Cohen_FelsonRoutine-Activities.pdf.

Cohen, Lawrence E., Marcus Felson and Kenneth C. Land. 1981. "Social Inequality and Predatory Criminal Victimization: An Exposition and a Test of a Formal Theory." *American Sociological Review* 46 (5):505-24.

Colangelo, Anthony J. 2011. "A Unified Approach to Extraterritoriality." *Virginia Law Review* 97: 1019-1109. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1762935.

Collins, Judith. 2014 (Posted on 28 May 2014). "Privacy Law Changes to Strengthen Protection." *The Beehive*. https://www.beehive.govt.nz/release/privacy-law-changes-strengthen-protection.

COMESA (Common Market for Eastern and Southern Africa). 2011. "Cybercrime Model Bill, 2011." In: *2011 Gazette 16,* 45-77. Lusaka: COMESA.

Commonwealth Secretariat. 2002. "Annex B – Computer and Computer Related Crimes Bill." In: *Model Law on Computer and Computer Related Crime*, 15-24. London: The Commonwealth. http://www.cybercrimelaw.net/documents/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf.

Commonwealth Secretariat. 2003. "Draft Model Law on Electronic Evidence," in: *2002 Meeting of Commonwealth Law Ministers and Senior Officials: Kingstown, St Vincent and the Grenadines, 18–21 November 2002*. London: Commonwealth Secretariat. http://www.oecd-ilibrary.org/commonwealth/governance/2002-meeting-of-commonwealth-law-ministers-and-senior-officials/draft-model-law-on-electronic-evidence_9781848598188-11-en.

Commonwealth Secretariat. 2014. "Annex A – The Commonwealth Working Group of Experts on Cybercrime Report to Commonwealth Law Ministers 2014." In: *Report of the Commonwealth Working Group of Experts on Cybercrime: Paper by the Commonwealth Secretariat*, i-57. London: The Commonwealth. http://thecommonwealth.org/sites/default/files/news-items/documents/Report_of_the_Commonwealth_Working_Group_of_Experts_on_Cybercrime_May_2014.pdf.

Commonwealth Network. "Commonwealth Secretariat." *Commonwealth Network*. http://www.commonwealthofnations.org/commonwealth/commonwealth-secretariat/.

Conklin, Kevin. 2017 (Posted in Jun. 2017). "The Petya Virus—Return of the Ransomware Attacks." *Information Management*. https://www.information-management.com/opinion/the-petra-virus-return-of-the-ransomware-attacks.

Constantin, Lucian. 2014 (Posted on 13 Jan. 2014). *"Target Point-of-sale Terminals were Infected with Malware."* PC World. http://www.pcworld.com/article/2087240/target-pointofsale-terminals-were-infected-with-malware.html.

Cook, David M. 2010. "Mitigating Cyber-Threats through Public-Private Partnerships: Low Cost Governance with High Impact Returns." In: *Proceedings of the 1st International Cyber Resilience Conference*, Perth, Western Australia, 23-24 Aug. pp. 22–30. Perth, Western Australia: Edith Cowan University. http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1002&context=icr.

CCDCOE (Cooperative Cyber Defence Centre of Excellence). 2015 (Posted on 20 Feb. 2015). "Mixed Feedback on the 'African Union Convention on Cyber Security and Personal Data Protection." *CCDCOE*. https://ccdcoe.org/mixed-feedback-african-union-convention-cyber-security-and-personal-data-protection.html.

Corera, Gordon. 2016 (Posted on 29 Jun. 2016). "CIA Taps Huge Potential of Digital Technology." *BBC News*. http://www.bbc.com/news/world-us-canada-36462056.

Corera, Gordon. 2017 (16 Jun. 2017). "NHS Cyber-Attack Was 'Launched from North Korea'," *BBC News*. http://www.bbc.com/news/technology-40297493.

Cottim, Armando. 2010. "Cybercrime, Cyberterrorism and Jurisdiction: An Analysis of Article 22 of the COE Convention on Cybercrime." *European Journal of Legal Studies* 2(3). http://www.ejls.eu/6/78UK.htm#_ftnref34.

Coughlin, Tom, Dennis Waid and Jim Porter. 2004 (Posted in April 2004). "The Disk Drive, 50 Years of Progress and Technology Innovation." In: *Computer Technology Review*. http://docplayer.net/25956649-The-disk-drive-50-years-of-progress-and-technology-innovation-the-road-to-2-billion-drives-tom-coughlin-dennis-waid-and-jim-porter.html.

Couldry, Nick. 2008. "Mediatization or Mediation? Alternative Understandings of the Emergent Space of Digital Storytelling." *New Media & Society* 10(3): 373-391. http://eprints.lse.ac.uk/50669/1/Couldry_Mediatization_or_mediation_2008.pdf.

Council of Europe. "Chart of Signatures and Ratifications of Treaty 185." Council of Europe. http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG.

Council of Europe. "Cybercrime Programme Office (C-PROC)." *Council of Europe*. http://www.coe.int/en/web/cybercrime/cybercrime-office-c-proc-.

Council of Europe. "Electronic Evidence Guide." *Council of Europe*. http://www.coe.int/en/web/octopus/home.

Council of Europe. "T-CY Reports." Council of Europe. http://www.coe.int/en/web/cybercrime/t-cy-reports.

Council of Europe. "Law Enforcement – Internet Service Provider Cooperation." *Council of Europe*. http://www.coe.int/en/web/cybercrime/lea-/-isp-cooperation.

Council of Europe. "Law Enforcement- Internet Service Provider Cooperation." *Council of Europe*. http://www.coe.int/en/web/cybercrime/lea-/-isp-cooperation

Council of Europe. "24/7 Points of Contact." *Council of Europe*. http://www.coe.int/en/web/cybercrime/resources.

Council of Europe. "Action against Cybercrime." *Council of Europe*. http://www.coe.int/en/web/cybercrime.

Council of Europe. "Cybercrime at COE Update April–June 2016." *Council of Europe*. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806931 47.

Council of Europe. "Cybercrime Convention Committee." *Council of Europe*. https://www.coe.int/en/web/cybercrime/tcy.

Council of Europe. "Global Action on Cybercrime: From GLACY to GLACY+." *Council of Europe*. http://www.coe.int/en/web/human-rights-rule-of-law/-/global-action-on-cybercrime-from-glacy-to-glacy-.

Council of Europe. "Global Project Cybercrime@Octopus." *Council of Europe*. http://www.coe.int/en/web/cybercrime/cybercrime-octopus.

Council of Europe. "Regional Project Cybercrime@EaP II." *Council of Europe*. http://www.coe.int/en/web/cybercrime/cybercrime-eap-ii.

Council of Europe. 2001. *Explanatory Report to the Convention on Cybercrime*. Budapest: Council of Europe. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce5b.

Council of Europe. 2007. "Questionnaire in preparation of the Conference." Paper prepared for the Octopus Interface Conference, "Conference on Cooperation against Cybercrime." Strasbourg, 11-12 June. http://www.coe.int/t/dghl/cooperation/economiccrime/Source/567-m-if%202008%20quest_en.doc.

Council of Europe. 2009. *Cybercrime: a Threat to Democracy, Human Rights and the Rule of Law.* Strasburg: Council of Europe.

Council of Europe. 2011. Article 15 –*Conditions and Safeguards under the Budapest Convention on Cybercrime: Discussion Paper with Contributions by Henrik Kaspersen (Netherlands) Joseph Schwerha (USA).* Strasbourg: Council of Europe. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802f2464.

Council of Europe. 2011. Law Enforcement Training Strategy. Strasbourg: Council of Europe. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802f6a34.

Council of Europe. 2012. *T-CY Guidance Note # 1 on the Notion of "Computer System": Article 1.a. of the Budapest Convention on Cybercrime.* Strasbourg: Council of Europe. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e79e6.

Council of Europe. 2013. *Capacity Building on Cybercrime: Discussion Paper.* Strasbourg: Council of Europe. http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/cyber%20CB_v1y.pdf.

Council of Europe. 2014. *Cybercrime Model Laws: Discussion Paper Prepared for the Cybercrime Convention Committee (T-CY).* Strasbourg: Council of Europe. http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Cybercrime@Octopus/Reports/2014_Zahid/3021_model_law_study_v15.pdf.

Council of Europe. 2015. *Cybercrime and Cybersecurity Strategies in the Eastern Partnership Region.* Bucharest: Council of Europe. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016803053d2.

Council of Europe, Octopus Cybercrime Community. "Advanced Course for Judges and Prosecutors." *Council of Europe.* http://www.coe.int/en/web/octopus/home.

Council of Europe, Project on Cybercrime and the Lisbon Network. 2009. "Cybercrime Training for Judges and Prosecutors: A Concept." Strasbourg: Council of Europe. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa3c3.

Council of Europe/Committee of Ministers. 1987. *Recommendation R (87)15 Regulating the Use of Personal Data in the Police Sector.* Strasbourg: Council of Europe. http://ec.europa.eu/justice/data-protection/law/files/coe-fra-rpt-2670-en-471.pdf.

Council of Europe/Economic Crime Division. 2008. *Guidelines for the cooperation of law enforcement and internet service providers against cybercrime.* Strasbourg: Council of Europe. http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Documents/Reports-Presentations/567_prov-d-guidelines_provisional2_3April2008_en.pdf.

Council of Europe/European Court of Human Rights. 2007. "Freedom of expression in Europe: Case-law concerning Article 10 of the European Convention on Human Rights." *Human Rights Files*, no. 18. Strasbourg: Council of Europe, European Court of Human Rights. http://www.echr.coe.int/LibraryDocs/DG2/HRFILES/DG2-EN-HRFILES-18(2007).pdf.

Council of Europe/European Court of Human Rights. 2011 (Updated in June 2015). *Internet: la jurisprudence de la CEDH.* Strasbourg: Council of Europe. http://www.echr.coe.int/Documents/Research_report_internet_FRA.pdf.

Council of the European Union. 2014. *EU Human Rights Guidelines on Freedom of Expression Online and Offline: Foreign Affairs Council meeting (Brussels, 12 May 2014).* Brussels: European Commission, Newsroom Editor. http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/EN/foraff/142549.pdf.

CJEU (Court of Justice of the European Union). 2015 (Posted on 6 Oct.2015). "The Court of Justice Declares That the Commission's US Safe Harbour Decision Is Invalid." *CJEU.* http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf.

Cox, Joseph. 2016 (Posted on 5 Jan. 2016). "The FBI's 'Unprecedented' Hacking Campaign Targeted over a Thousand Computers." *Motherboard.* http://motherboard.vice.com/read/the-fbis-unprecedented-hacking-campaign-targeted-over-a-thousand-computers.

Crawford, Jamie. 2016 (Posted on 13 Jan. 2016). "Kerry Tells Iran in Long Day of Calls: This Can be 'a Good Story for Both of Us'." *CNN.* http://www.cnn.com/2016/01/13/politics/john-kerry-iran-zarif-sailors/.

Crumbley, Larry, Lester E. Heitger and G. Stevenson Smith. 2005. *Forensic and Investigative Accounting* (2nd Edition). Washington D.C.: CCH.

Cuomo, Andrew M. and Benjamin M. Lawsky. 2014. *Report on Cyber Security in the Banking Sector.* New York: New York State Department of Financial Services. http://www.dfs.ny.gov/reportpub/dfs_cyber_banking_report_052014.pdf.

Cyber Crime and Forensics Blog. 2009 (Posted on 26 Feb. 2009). "Data Diddling." *Cyber Crime and Forensics Blog.* http://cybercrimeandforensic.blogspot.com/2009/02/data-diddling.html.

Cyber Security Law & Policy. 2016 (Posted on 23 Feb. 2016). "Actual Order Compelling Apple, Inc. to Assist Agents in Search of iPhone." *Cybersecuritylaw.* http://blog.cybersecuritylaw.us/2016/02/23/actual-order-compelling-apple-inc-to-assist-agents-in-search-of-iphone/.

Cyberoam. 2012 (Posted on 6 Dec. 2012). "Is Bitcoin Turning into a Cyber Crime Currency?" *Cyberoam*. https://web.archive.org/web/20160404100125/http://www.cyberoam.com/blog/is-bitcoin-turning-into-a-cyber-crime-currency-2/.

D

Daily News. 2015 (Posted on 20 Mar. 2015). "Approved Article Gives Turkish Gov't Power to Shut Down Websites in Four Hours." *Daily News*. http://www.hurriyetdailynews.com/approved-article-gives-turkish-govt-power-to-shut-down-websites-in-four-hours.aspx?pageID=238&nID=79941&NewsCatID=339.

Day, Matt. 2017 (Posted on 14 May 2017). "Microsoft Criticizes Government Creation of Hacking Tools Used in Global Cyberattack." *Seattle Times*. http://www.seattletimes.com/business/microsoft/microsoft-criticizes-government-creation-of-hacking-tools-used-in-global-cyberattack/.

Deibert, Ronald. 2012. "The Growing Dark Side of Cyberspace (…and What to Do About It)." *Penn State Journal of Law & International Affairs* 1(2). http://elibrary.law.psu.edu/cgi/viewcontent.cgi?article=1012&context=jlia.

Deleon, Nicholas. 2008 (Posted on 26 Mar. 2008). "Phishing Scam Targeting Facebook Users." *TechCrunch.com*. http://techcrunch.com/2008/03/26/phishing-scam-targeting-facebook-users/.

Deloitte CFO. 2013 (Posted on 7 Jul. 2013). "Eight Ways to Move Toward a Culture of Compliance." *Wall Street Journal*. http://deloitte.wsj.com/cfo/2013/06/07/toward-a-culture-of-compliance-eight-initiatives-ccos-can-lead/.

DeYoung, Karen. 2016 (Posted on 13 Jan. 2016). "Intense Diplomacy between Secretary of State Kerry and His Iranian Counterpart to Secure Sailors." *Washington Post*. https://www.washingtonpost.com/news/checkpoint/wp/2016/01/13/intense-diplomacy-between-secretary-of-state-kerry-and-his-iranian-counterpart-to-secure-sailors-release/.

Di Lorenzo, Vincent. 1986. "Public Confidence and the Banking System: The Policy Basis for Continued Separation of Commercial and Investment Banking." *American Law Review 35*. http://www.stjohns.edu/sites/default/files/documents/law/dilorenzo-public_confidence_policy_basis.pdf.

DigiCert. "The Math Behind Estimations to Break a 2048-bit Certificate." *DigiCert*. https://www.digicert.com/TimeTravel/math.htm.

Digital Watch. "Geneva Internet Platform." *Digital Watch*. http://digitalwatch.giplatform.org/instruments/agreement-cooperation-combating-offences-related-computer-information-commonwealth.

Douglas, Thomas and Brian D. Loader, eds. 2000. "Introduction–Cyber Crime: Law Enforcement, Security and Surveillance in the Information Age." In: Douglas, Thomas and Brian D. Loader, eds. 2000. *Cyber crime: Law enforcement, security and surveillance in the information age*. London: Routledge.

Dotzauer, Erwin. 2014 (Posted on 3 Nov. 2014). "UNODC – Comprehensive Study on Cybercrime." *Cybersecurity Capacity Portal*. https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/unodc-comprehensive-study-cybercrime.

Downing, Richard W. 2005. "Shoring Up the Weakest Link: What Lawmakers Around the World Need to Consider in Developing Comprehensive Laws to Combat Cybercrime." *Columbia Journal of Transnational Law* 43(3): 705.

Doyle, Charles. 2016 (Posted on 18 May 2016). "RICO: A Brief Sketch." US Congressional Research Service (CRS), no. 96-950. https://fas.org/sgp/crs/misc/96-950.pdf.

Dubber, Markus D. 2013 (Posted on 3 Jul. 2013). "Ultima Ratio as Caveat Dominus: Legal Principles, Police Maxims, and the Critical Analysis of Law." *SSRN (Social Science Research Network)*. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2289479.

Dunham, Jennifer, Bret Nelson and Elen Aghekyan. 2015. *Freedom of the Press 2015*. Washington, D.C.: Freedom House. https://freedomhouse.org/sites/default/files/FreedomofthePress_2015_FINAL.pdf.

Dutton, William H. Anna Dopatka, Michael Hills, Ginette Law & Victoria Nash. 2011. *Freedom of Connection, Freedom of Expression; the Changing Legal and Regulatory Ecology Shaping the Internet*. Paris: UNESCO. http://unesdoc.unesco.org/images/0019/001915/191594e.pdf.

Dutton, William H., Ginette Law, Gillian Bolsover and Soumitra Dutta. 2013. *The Internet Trust Bubble: Global Values, Beliefs and Practices*. Geneva: WEF (World Economic Forum). http://www3.weforum.org/docs/WEF_InternetTrustBubble_Report2_2014.pdf.

E

Eadicicco, Lisa. 2015 (Posted on 19 Oct. 2015). "Hundreds of Apps Have Been Banned from Apple's App Store for Spying on Your Personal Information." *Business Insider*. http://www.businessinsider.com/apple-removes-apps-youmi-sdk-personal-information-2015-10.

Edwards, Julia. 2016 (Posted on 22 Apr. 2016). "FBI Paid More Than $1.3 Million to Break into San Bernardino iPhone." *Reuters*. http://www.reuters.com/article/us-apple-encryption-fbi-idUSKCN0XI2IB.

Effross, Walter A. 1997. "High-Tech Heroes, Virtual Villains and Jacked-In Justice: Visions of Law and Lawyers in Cyberpunk Science Fiction." *Buffalo Law Review* 45 (3):931-974.

Electronic Frontier Foundation. "The Playpen Cases: Frequently Asked Questions The Basics." *Electronic Frontier Foundation*. https://www.eff.org/pages/playpen-cases-frequently-asked-questions#howmanycases.

Emerging Technology from the arXiv. 2017 (Posted on 5 Apr. 2017). "Intelligent Machines Quantum Computing Now Has a Powerful Search Tool." *MIT Technology Review*. https://www.technologyreview.com/s/604068/quantum-computing-now-has-a-powerful-search-tool/.

End Stalking in America, Inc. "Building Your Case." *End Stalking in America, Inc*. http://www.esia.net/Building_your_Case.htm.

Engelbrekt, Kjell. 2016. *High-Table Diplomacy: The Reshaping of International Security Institutions*. Washington, DC: Georgetown University Press.

Eskola, Marko. 2012. "From Risk Society to Network Society: Preventing Cybercrimes in the 21st Century." *Journal of Applied Security Research* 7(1): 122 –150.

Etter, Barbara. 2001. *The forensic challenges of e-crime*. Marden: ACPR (Australasian Centre for Policing Research).

EuropaForum. 2016 (Posted on 13 Sep. 2016). *"Traités et Affaires institutionnelles: Respect de l'état de droit – La Commission, soutenue par une majorité du Parlement européen, maintient la pression sur Varsovie." EuropaForum*. http://www.europaforum.public.lu/fr/actualites/2016/09/pe-pologne-etat-de-droit/index.html.

EC (European Commission). 2010. "A Comprehensive Approach on Personal Data Protection in the European Union." COM (2010) 609 Final. Brussels: EC. http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf.

EC. 2010. "The EU Internal Security Strategy in Action: Five steps towards a more secure Europe." COM (2010) 673 Final. Brussels: EC. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52010DC0673&from=EN.

EC. 2015 (Posted on 14 Dec. 2015)."Roadmap." *Public Private Partnership on Cybersecurity*. http://ec.europa.eu/smart-regulation/roadmaps/docs/2015_cnect_004_cybersecurity_en.pdf.

EC. 2016 (Posted on 2 Feb. 2016). "EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield." *European Commission –Press Release*. http://europa.eu/rapid/press-release_IP-16-216_en.htm.

EC. 2016 (Posted on 12 Jul. 2016). "EU-US Privacy Shield: Frequently Asked Questions," *Fact Sheet, European Commission*. http://europa.eu/rapid/press-release_MEMO-16-2462_en.htm.

EC. "Eastern Partnership, Migration and Home Affairs." *European Commission*. https://ec.europa.eu/home-affairs/what-we-do/policies/international-affairs/eastern-partnership_en.

EC. "Public Consultation on the Public-Private Partnership on Cybersecurity and Possible Accompanying Measures." *European Commission*. https://ec.europa.eu/digital-single-market/en/news/public-consultation-public-private-partnership-cybersecurity-and-possible-accompanying-measures.

EC. "DG Connect." *European Commission*. https://ec.europa.eu/digital-single-market/dg-connect.

EC. "Horizon 2020." *European Commission*. https://ec.europa.eu/programmes/horizon2020/.

EC. "Digital Single Market: Bringing Down Barriers to Unlock Online Opportunities." *European Commission*. http://ec.europa.eu/priorities/digital-single-market/.

EC, Commissioner. "Digital Single Market." *European Commission*. http://ec.europa.eu/priorities/digital-single-market/.

EDRi (European Digital Rights). 2008 (Posted on 17 Dec. 2008). "Bulgarian Court Annuls a Vague Article of the Data Retention Law." *EDRi*. https://edri.org/edri-gramnumber6-24bulgarian-administrative-case-data-retention/.

EDRi. 2010 (Posted on 10 Mar. 2010). "German Federal Constitutional Court Rejects Data Retention Law." *EDRi*. https://edri.org/edrigramnumber8-5german-decision-data-retention-unconstitutional/.

EU Agency for Fundamental Rights. 2014. "Violence Against Women: An EU-wide Survey." *EU Agency for Fundamental Rights*. http://fra.europa.eu/en/publication/2014/violence-against-women-eu-wide-survey-main-results-report.

European Parliament. 2015 (Posted on 7 Dec. 2015). "MEPs Close Deal with Council on First Ever EU Rules on Cybersecurity." *European Parliament –Press Release*. http://www.europarl.europa.eu/news/en/news-room/20151207IPR06449/MEPs-close-deal-with-Council-on-first-ever-EU-rules-on-cybersecurity.

EUROPOL (European Police Office). 2014 (Posted on 9 May 2014). "Worldwide Operation against Cybercriminals." *EUROPOL*. https://www.europol.europa.eu/content/worldwide-operation-against-cybercriminals.

EUROPOL. 2015. *The Internet Organised Crime Threat Assessment (IOCTA) 2015.* The Hague: EUROPOL. https://www.europol.europa.eu/sites/default/files/publications/europol_iocta_web_2015.pdf.

EUROPOL. "Europol Supports Huge International Operation to Tackle Organised Crime." *Europol*. https://www.europol.europa.eu/content/europol-supports-huge-international-operation-tackle-organised-crime.

EUROPOL. "European Cybercrime Centre- EC3." *Europol*. https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3.

EUROPOL. "Combating Cybercrime in a Digital Age." *Europol, European Cybercrime Centre (EC3)*. https://www.europol.europa.eu/ec3.

Europol. "Joint Cybercrime Action Taskforce (J-CAT)." *Europol, European Cybercrime Centre (EC3)*. https://www.europol.europa.eu/ec3/joint-cybercrime-action-taskforce-j-cat.

European Union Agency for Network and Information Security (ENISA). "National Cyber Security Strategies in the World." *ENISA*. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world.

EUR-Lex. "Digital Agenda for Europe." *EUR-Lex*. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV:si0016.

EUROJUST (European Union's Judicial Cooperation Unit). 2015. *Operation BlackShades: An Evaluation*. Hague: *EUROJUST*. https://www.gccs2015.com/sites/default/files/documents/Bijlage%202%20-%20Eurojust%20(10%2004%2015)%20Blackshades-Case-Evaluation.pdf.

Eurojust. "History of Eurojust." *Eurojust*. http://www.eurojust.europa.eu/about/background/Pages/history.aspx.

Eurojust. "Mission and Tasks." *Eurojust*. http://www.eurojust.europa.eu/about/background/Pages/mission-tasks.aspx.

European Cybercrime Training and Education Group (ECTEG). "European Cybercrime Training and Education Group." *European Cybercrime Training and Education Group*. http://www.ecteg.eu.

European Network of Living Labs." European Network of Living Labs." *European Network of Living Labs*. http://www.openlivinglabs.eu/.

Evans, Martin. 2017 (Posted on 19 Jan. 2017). "Fraud and Cyber Crime are Now the Country's Most Common Offences." *Telegraph*. http://www.telegraph.co.uk/news/2017/01/19/fraud-cyber-crime-now-countrys-common-offences/.

Evening Standard. 2011 (Posted on 8 Nov. 2011). "MP Demands Law to Force Internet Providers to Remove Gang Videos." *Evening Standard –News*. http://www.standard.co.uk/news/mp-demands-law-to-force-internet-providers-to-remove-gang-videos-6365780.html.

Executive Office of the President. 2014. *Big Data: Seizing Opportunities, Preserving Values.* Washington D.C.: The White House https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf.

Executive Office of the President, President's Council of Advisors on Science and Technology. 2014. *Big Data and Privacy: A Technological Perspective*. Washington D.C.: The White House. https://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf.

Exum, Jelani Jefferson. 2010. "Making the Punishment Fit the (Computer) Crime: Rebooting Notions of Possession for the Federal Sentencing of Child Pornography Offenses." *Richmond Journal of Law and Technology* 16(3). http://jolt.richmond.edu/v16i3/article8.pdf.

F

Fafinski, Stefan Frederick. 2008. *Computer Use and Misuse: The Constellation of Control*. The University of Leeds, School of Law. http://etheses.whiterose.ac.uk/2273/1/Fafinski_S_Law__PhD_2008.pdf.

Farbiarz, Michael. 2016. "Accuracy and Adjudication: The Promise of Extraterritorial Due Process." *Columbia Law Review* 116(3).

FBI (Federal Bureau of Investigation). 2014 (Posted on 19 May. 2014). "International Blackshades Malware Takedown-Coordinated Law Enforcement Actions Announced." FBI. https://www.fbi.gov/news/stories/2014/may/international-blackshades-malware-takedown/international-blackshades-malware-takedown.

FBI. "National Cyber Investigative Joint Task Force." *FBI*. https://www.fbi.gov/investigate/cyber/national-cyber-investigative-joint-task-force.

Feigenbaum, Joan, Aaron Johnson & Paul Syverson. 2006. "A Model of Onion Routing with Provable Anonymity." *Financial Cryptography & Data Security*. http://www.cs.yale.edu/homes/jf/FJS.pdf.

Feinberg, Joel and Robert P. George. 1990. "Crime and Punishment: Moralistic Liberalism and Legal Moralism: Harmless Wrongdoing: The Moral Limits of the Criminal Law." *Michigan Law Review 88:* 1415.

Ferzan, Kimberly Kessler. 2013. "Prevention, Wrongdoing and the Harm Principle's Breaking Point." *Ohio State Journal of Criminal Law* 10(2): 679 –695. http://moritzlaw.osu.edu/students/groups/osjcl/files/2013/03/25.-Ferzan.pdf.

Fidler, Mailyn. 2015 (Posted on 22 Jun. 2015). "The African Union Cybersecurity Convention: A Missed Human Rights Opportunity." *Council of Foreign Relations Blog*. http://blogs.cfr.org/cyber/2015/06/22/the-african-union-cybersecurity-convention-a-missed-human-rights-opportunity/

Figliola, Patricia Moloney. 2009. *Spyware: Background and Policy Issues for Congress*. Washington D.C.: CRS (Congressional Research Service). https://ia601307.us.archive.org/0/items/135973SpywareBackgroundandPolicyIssuesforCongress-crs/135973%20Spyware_%20Background%20and%20Policy%20Issues%20for%20Congress.pdf.

FSIAC. "Financial Services-ISAC." *Financial Sector Information Sharing and Analysis Center*. http://www.fsisac.com.

Finkle, Jim. 2016 (Posted on 31 Aug. 2016). "SWIFT Discloses More Cyber-Thefts, Pressures Banks on Security." *Reuters*. http://www.reuters.com/article/us-cyber-heist-swift-idUSKCN11600C.

Finklea, Kristin and Catherine A. Theohary. 2015. *Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement*. Washington D.C.: CRS (Congressional Research Service). https://www.fas.org/sgp/crs/misc/R42547.pdf.

Flanagan, Anne. 2005. "The Law and Computer Crime: Reading the Script of Reform." *International Journal of Law & Information Technology* 13(1).

Flitter, Emily. 2013 (Posted on 29 May. 2013). "U.S. Accuses Currency Exchange of Laundering $6 Billion." *Reuters*. http://www.reuters.com/article/2013/05/29/net-us-cybercrime-libertyreserve-charges-idUSBRE94R0KQ20130529.

Flynn, Mary Kathleen. 2002 (Posted on 8 Nov. 2002). "ISACs, Infragard and ECTF: Safety in Numbers." *CSO*. http://www.csoonline.com/article/2113264/security-leadership/isacs--infragard--and-ectf--safety-in-numbers.html.

Forensic Colleges & Universities. "10 Modern Forensic Science Technologies." *Forensic Colleges & Universities*. http://www.forensicscolleges.com/blog/resources/10-modern-forensic-science-technologies.

Forte, Dario. 2002. "Analyzing the Difficulties in Backtracing Onion Router Traffic." *International Journal of Digital Evidence* 1(3). https://www.utica.edu/academic/institutes/ecii/publications/articles/A04AA07D-D4B8-8B5F-450484589672E1F9.pdf.

Fox-Brewster, Thomas. "An NSA Cyber Weapon Might Be Behind A Massive Global Ransomware Outbreak." *Forbes*. https://www.forbes.com/sites/thomasbrewster/2017/05/12/nsa-exploit-used-by-wannacry-ransomware-in-global-explosion/#514a4d77e599.

Foxx, Chris. 2017 (Posted on 14 May 2017). "Global Cyber-attack: Security Blogger Halts Ransomware 'by Accident'." *BBC News*. http://www.bbc.com/news/technology-39907049.

Franceschi-Bicchierai, Lorenzo. 2015 (Posted on 4 May 2015). "Love Bug: The Virus That Hit 50 Million People Turns 15." *Motherboard*. http://motherboard.vice.com/read/love-bug-the-virus-that-hit-50-million-people-turns-15.

Fujikawa, Megumi. 2014 (Posted on 22 Oct. 2014). "Google Japan Case Raises Issue of 'Right to Be Forgotten'." *Wall Street Journal*. http://www.wsj.com/articles/google-japan-case-raises-privacy-issues-1413981229.

Fuller, Kathleen E. 2001. "ICANN: The Debate over Governing the Internet." *Duke Law and Technology Review* 1(1). http://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1000&context=dltr.

Furnell, Steven. 2002. *Cyber crime: Vandalizing the information society.* London: Addison Wesley.

G

G8. 1997 (Posted on 10 Dec. 1997). "The Washington Communiqué." Meeting of Justice and Interior Ministers of the Eight. https://www.justice.gov/sites/default/files/ag/legacy/2004/06/08/97Communique.pdf.

Galeote, Rocio. 2015 (Posted on 30 Jul. 2015). "South Korea: Major Health Data Breach Hits Sector 'Weak' in Compliance." *Data Guidance*. http://www.dataguidance.com/dataguidance_privacy_this_week.asp?id=4621.

Gallagher, Harold, Wade McMahon and Ron Morrow. 2014. *Cyber Security: Protecting the Resilience of Canada's Financial System*. Ottawa: Bank of Canada. http://www.bankofcanada.ca/wp-content/uploads/2014/12/fsr-december14-morrow.pdf.

Gallagher, Kevin M. 2014 (Posted on 18 Jun. 2014). "Private Spies Deserve More Scrutiny." *Huffington Post*. http://www.huffingtonpost.com/kevin-m-gallagher/private-sector-surveillance_b_5171750.html.

Garofalo, James. 1987. "Reassessing the Lifestyle Model of Criminal Victimization." In: Michael R. Gottfredson and Travis Hirschi, eds. 1987. *Positive criminology:* 23-42. Thousand Oaks: Sage Publications, Inc.

Gemalto. 2015. *2015 First Half Review: Findings from the Breach Level Index*. North Holland, Netherlands: Gemalto NV. http://www.gemalto.com/brochures-site/download-site/Documents/Gemalto_H1_2015_BLI_Report.pdf.

Geradin, Damien, Marc Reysen & David Henry. 2008. "Extraterritoriality, Comity and Cooperation in EC Competition Law." *SSRN*. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1175003.

Gercke, Marco. 2004. "The Implementation of the Cybercrime Convention –Procedural Law." In: *Multimedia und Recht:* 801 to 806.

Gercke, Marco. 2005. "Phishing and Identity Theft." *Computer und Recht:* 606-612.

Gercke, Marco. 2007. *Internet-Related Identity Theft: A Discussion Paper by Marco Gercke (Germany).* Strasbourg: Council of Europe. http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/cy%20activity_events_on_identity_theft/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf.

Gercke, Marco. 2008. "Challenge of Fighting Cybercrime."In: *Multimedia und Recht:* 291 –298.

Gercke, Marco. 2008. "The Council of Europe Guidelines for the Cooperation between Law Enforcement Agencies and Internet Service Providers against Cybercrime." *Computer Law Review International:* 91-101.

Gercke, Marco. 2009. "The Role of Internet Service Providers in the Fight against Child Pornography." *Computer Law Review International:* 65 –72.

Gercke, Marco. 2009. *Understanding Cybercrime: A Guide for Developing Countries.* Geneva: ITU. http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf.

Gercke, Marco. 2011. "Legal Approaches to Criminalize Identity Theft." In: UNODC. *Handbook on Identity-related Crime,* 1 –54. New York: UN. https://www.unodc.org/documents/treaties/UNCAC/Publications/Handbook_on_ID_Crime/10-57802_ebooke.pdf.

Gercke, Marco. 2012. *Understanding Cybercrime: Phenomena, Challenges and Legal Response.* Geneva: ITU. http://www.itu.int/en/ITU-D/Cybersecurity/Documents/CybcrimeE.pdf.

Gercke, Marco. 2014. *Understanding Cybercrime: Phenomena, Challenges and Legal Response* (November 2014). Geneva: ITU. http://www.itu.int/en/ITU-D/Cybersecurity/Documents/cybercrime2014.pdf.

Germano, Judith H. 2014. *Cybersecurity Partnerships: A New Era of Public-Private Collaboration.* New York: New York University School of Law/Center on Law and Security. http://www.lawandsecurity.org/Portals/0/Documents/Cybersecurity.Partnerships.pdf.

Gibson Dunn. 2016. *Cybersecurity and Data Privacy Outlook and Review: 2016.* Los Angeles: Gibson, Dunn & Crutcher LLP. http://www.gibsondunn.com/publications/documents/Cybersecurity-and-Data-Privacy-Outlook-and-Review--2016.pdf.

Gibbon, Edward. 1960. *The Decline and Fall of the Roman Empire.* New York: Harcourt, Brace.

Gilbert, Françoise. 2017. Global Privacy & Security Law. Palo Alto: Wolters Kluwer.

Giordano, Scott M. 2004. "Electronic Evidence and the Law." *Information Systems Frontiers* 6(2): 161 –174.

Gladyshev, Pavel and Ahmed Patel. 2005. "Formalizing Event Time Bounding in Digital Investigations." *International Journal of Digital Evidence* 4(2). https://www.utica.edu/academic/institutes/ecii/publications/articles/B4A90270-B5A9-6380-68863F61C2F7603D.pdf.

Global Monitoring and ECPAT International. 2016. *Status of Action against Commercial Sexual Exploitation of Children: Israel (2016)*. Bangkok: ECPAT International.

Global Partners Digital Development House. 2015. GCCS2015 Collated Training Summaries. London: Global Partners Digital Development House. http://www.gp-digital.org/wp-content/uploads/pubs/GCCS2015%20Collated%20Webinar%20Summaries%20final.pdf.

Goel, Vindu. 2015 (Posted on 14 Oct. 2015). "Encryption Is More Important, and Easier, Than Ever By." *New York Times*. http://bits.blogs.nytimes.com/2015/10/14/encryption-is-more-important-and-easier-than-ever/?_r=0.

Goel, Vindu & Nicole Perlroth. 2016 (Posted on 14 Dec. 2016). "Yahoo Says 1 Billion User Accounts Were Hacked." *New York Times*. https://www.nytimes.com/2016/12/14/technology/yahoo-hack.html?mcubz=3.

Goger, Thomas. 2016. "Cross-border Cybercrime Investigations – Making MLATs Work". *Mimeo*.

Goodin, Dan. 2014 (Posted on 18 Nov. 2014). "WhatsApp Brings Strong End-to-end Frypto to the Masses." *Quora*. https://www.quora.com/How-secure-is-WhatsApps-new-end-to-end-encryption.

Goodman, Marc. D. 1997. "Why the Police don't care about Computer Crime." *Harvard Journal of Law & Technology* 10(3): 465–494. http://jolt.law.harvard.edu/articles/pdf/v10/10HarvJLTech465.pdf.

Goodman, Marc D. and Susan W. Brenner. 2002. "The Emerging Consensus on Criminal Conduct in Cyberspace." *UCLA Journal of Law and Technology* 10(2): 139–223.

Goodno, Naomi Harlin. 2007. "Cyberstalking, a New Crime: Evaluating the Effectiveness of Current State and Federal Laws." *Missouri Law Review 72*. http://scholarship.law.missouri.edu/cgi/viewcontent.cgi?article=3985&context=mlr.

Gordon, Gary R., Chet D. Hosmer, Christine Siedsma and Don Rebovich. 2002. *Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime*. Rockville: NCJRS (National Criminal Justice Reference Service). https://www.ncjrs.gov/pdffiles1/nij/grants/198421.pdf.

Gordon, Mark. 2002. "Ideas Shoot Bullets: How the RICO Act Became a Potent Weapon in the War Against Organized Crime," Concept, Vol. 26, (2002). https://concept.journals.villanova.edu/article/view/312/275.

Gordon, Sarah and Richard Ford. 2006. "On the Definition and Classification of Cybercrime." *Journal of Computer Virology* 2: 13-20. https://pdfs.semanticscholar.org/12f8/7da74f91c7bfac67b6e83213fefe2c08bb67.pdf.

Gottfredson, Michael R. 1984. "Victims of Crime: The Dimensions of Risk." *Home Office Research Study No.18.* London: Her Majesty's Stationer. http://webarchive.nationalarchives.gov.uk/20110218135832/rds.homeoffice.gov.uk/rds/pdfs05/hors81.pdf.

Gov.uk. "Cabinet Office." *Gov.uk.* https://www.gov.uk/government/organisations/cabinet-office.

Gov.uk. "Department for Business, Energy and Industrial Strategy (BEIS)." *Gov.uk.* https://www.gov.uk/government/organisations/department-for-business-innovation-skills

Gov.uk. "Department for Culture, Media and Sport." *Gov.uk.* https://www.gov.uk/government/organisations/department-for-culture-media-sport.

Gov.uk. "Foreign and Commonwealth Office." *Gov.uk.* https://www.gov.uk/government/organisations/foreign-commonwealth-office.

Gov.uk. "Home Office." *Gov.uk.* https://www.gov.uk/government/organisations/home-office.

Gov.uk. "Ministry of Defence." *Gov.uk.* https://www.gov.uk/government/organisations/ministry-of-defence.

Government of the United Kingdom. 2013 (Posted on 23 Mar. 2013). "Government Launches Information Sharing Partnership on Cyber Security." *Government of the United Kingdom/Press Release.* https://www.gov.uk/government/news/government-launches-information-sharing-partnership-on-cyber-security.

Gowen, Annie. 2016 (Posted on 28 Jan. 2016). "India, Egypt Say No Thanks to Free Internet from Facebook". *The Washington Post.* https://www.washingtonpost.com/world/asia_pacific/india-egypt-say-no-thanks-to-free-internet-from-facebook/2016/01/28/cd180bcc-b58c-11e5-8abc-d09392edc612_story.html.

Grabosky, Peter. 2000. "Cyber Crime and Information Warfare." Paper presented at the Australian Institute of Criminology Conference, "Transnational Crime," Canberra, 9-10 Mar. http://aic.gov.au/media_library/conferences/transnational/grabosky.pdf.

Gray, John and G.W. Smith, eds. 1991. *J.S. Mill's On Liberty in Focus* (1st Edition). New York: Routledge.

Gray, Laura. 2016 (Posted on 25 Mar. 2016). "Does Uganda Have More Mobile Phones Than Light Bulbs?" *BBC News*. http://www.bbc.com/news/magazine-35883649.

Green, Thomas. 2011 (Posted on 12 Mar. 2001). "FBI Magic Lantern reality check." *Register*. www.theregister.co.uk/2001/12/03/fbi_magic_lantern_reality_check/.

Greenberg, Andy. 2014 (25 Nov. 2014). "Hacker Lexicon: What Is End-to-End Encryption?" *Wired*. https://www.wired.com/2014/11/hacker-lexicon-end-to-end-encryption/.

Greenberg, Andy. 2016 (Posted on 29 May 2016). ""Silk Road Creator Ross Ulbricht Sentenced to Life in Prison." *Wired*. https://www.wired.com/2015/05/silk-road-creator-ross-ulbricht-sentenced-life-prison/.

Greenberg, Andy. 2016 (Posted on 6 Oct. 2016). "Judges Question Ross Ulbricht's Life Sentence in Silk Road Appeal." *Wired*. https://www.wired.com/2016/10/judges-question-ulbrichts-life-sentence-silk-road-appeal/.

Greenberg, Andy. 2017 (Posted on 14 Apr. 2017). "Major Leak Suggests NSA Was Deep in Middle East Banking System." *Wired*. https://www.wired.com/2017/04/major-leak-suggests-nsa-deep-middle-east-banking-system/.

Greene, Thomas C. 2001 (Posted on 3 Dec. 2001). "FBI 'Magic Lantern' reality check." *The Register*. http://www.theregister.co.uk/2001/12/03/fbi_magic_lantern_reality_check/.

Greenleaf, Graham and George Tian. 2013. "China Expands Data Protection through 2013 Guidelines: A 'Third Line' for Personal Information Protection (With a Translation of the Guidelines)." *Privacy Laws & Business International Report Issue* 122. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2280037.

Greenwald, Glenn. 2014. *No Place to Hide: Edward Snowden, the NSA and the Surveillance State*. New York: Metropolitan Books.

Griffin, Andrew. 2016 (Posted on 31 Dec. 2016). "Investigatory Powers Act Goes into Force, Putting UK Citizens under Intense New Spying Regime." *Independent*. http://www.independent.co.uk/life-style/gadgets-and-tech/news/investigatory-powers-act-bill-snoopers-charter-spying-law-powers-theresa-may-a7503616.html.

Griffin, J.P. 1999. "Extraterritoriality in US and EU Antitrust Enforcement," *Antitrust Law Journal* 67.

Guinchard, Audrey. 2008. "Cybercrime: The Transformation of Crime in the Information Age." *Information, Communication and Society* 11 (7):1030-1032.

Gupta, Gaurav, Chandan Mazumdar & M. S. Rao. 2004. "Digital Forensic Analysis of E-Mails: A Trusted E-Mail Protocol." *International Journal of Digital Evidence* 2(4). https://utica.edu/academic/institutes/ecii/publications/articles/A0B4342D-E76E-F8F2-AC926AB64EC719B8.pdf.

Gupta, Mayank R., Michael D. Hoeschele and Marcus K. Rogers. 2006. "Hidden Disk Areas: HPA and DCO." *International Journal of Digital Evidence* 5(1). https://www.utica.edu/academic/institutes/ecii/publications/articles/EFE36584-D13F-2962-67BEB146864A2671.pdf.

Gupta, Sunil Kumar. 2000. "Extradition Law and the International Criminal Court." *Berkeley Journal of Criminal Law* 3. http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1072&context=bjcl.

H

Halderman, J. Alex, Seth D. Schoen, Nadia Heninger, William Clarkson, William Paul, Joseph A. Calandrino, Ariel J. Feldman, Jacob Appelbaum and Edward W. Felten. 2008. "Lest we Remember: Cold Boot Attacks on Encryption keys." *Communications of the ACM* 52(5): 91-98. https://www.usenix.org/legacy/event/sec08/tech/full_papers/halderman/halderman.pdf.

Hall, Gregory A. and Wilbon P. Davis. 2005. "Towards Defining the Intersection of Forensic and Information Technology." *International Journal of Digital Evidence* 4(1). https://www.utica.edu/academic/institutes/ecii/publications/articles/B49F0174-F1FB-FE05-EBBB4A8C87785039.pdf.

Hannan, Mathew. 2004 (Posted on 25 Nov. 2004). "To Revisit: What is Forensic Computing." Paper presented at the 2nd Australian Computer Network & Information Forensics Conference, Perth, Western Australia.https://conferences.ecu-sri.org/proceedings/2004/forensics04/Hannan.pdf.

Hargrave, Vic. 2012 (Posted on 17 Jun. 2012). "Hacker, Hacktivist or Cybercriminal?" *Trend Micro/Simply Security*. http://blog.trendmicro.com/whats-the-difference-between-a-hacker-and-a-cybercriminal/.

Harris, Aisha. 2014 (Posted on 17 Dec. 2014). "Sony Really Should Release the Interview Online, and Soon." *Slate*. http://www.slate.com/blogs/browbeat/2014/12/17/the_interview_pulled_from_theaters_due_to_north_korea_s_apparent_data_hack.html.

Harris, Kamala. 2014. 2014 California Data Breach Report. California Office of the Attorney General. https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/2014data_breach_rpt.pdf.

Harrison, Warren, George Heuston, Mark Morrissey, David Aucsmith, Sarah Mocas and Steve Russelle. 2002."A Lesson Learned Repository for Computer Forensics." *International Journal of Digital Evidence* 1(3). https://www.dfrws.org/2002/papers/Papers/Warren_Harrison.pdf.

Hern, Alex. 2016 (Posted on 28 Jun. 2016). "Google Says Machine Learning Is the Future. So I Tried It Myself." *Guardian*. https://www.theguardian.com/technology/2016/jun/28/google-says-machine-learning-is-the-future-so-i-tried-it-myself/.

Ho, Michael, Joyce Hung and Michael Hasnick. 2015. *The Carrot and the Stick: Innovation versus Anti-Piracy Enforcement*. Redwood City: The Copia Institute. https://copia.is/wp-content/uploads/2015/10/COPIA-The-Carrot-Or-The-Stick.pdf.

Hoboken, Joris van. 2012. *Search Engine Law and Freedom of Expression: A European Perspective*. New York: Wolters Kluwer Law & Business, Kluwer Law International.

Hogan Lovells. 2014. "Technology Neutrality in Internet, Telecoms and Data Protection Regulation." *Hogan Lovells Global Media and Communications Quarterly*. http://www.hoganlovells.com/files/Uploads/Documents/8%20Technology%20neutrality%20in%20Internet.pdf.

Homeland Security News Wire. 2011 (Posted on 19 Apr. 2011). "An Electronic Trail for Every Crime." *Homeland Security News Wire*. http://www.homelandsecuritynewswire.com/electronic-trail-every-crime.

Hosein, Gus & Caroline Wilson Palow. 2013. "The Second Wave of Global Privacy Protection: Modern Safeguards for Modern Surveillance: An Analysis of Innovations in Communications Surveillance Techniques." *Ohio State Law Journal* 74.

Hosmer, Chet. 2002. "Proving the Integrity of Digital Evidence with Time." *International Journal of Digital Evidence* 1(1). https://www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf.

Hostetler, Baker. 2015. "International Compendium of Data Privacy Laws." BakerLaw.com. http://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/International-Compendium-of-Data-Privacy-Laws.pdf.

Houle, Kevin J. and George M. Weaver. 2001. *Trends in Denial of Service Attack Technology*. Pittsburgh: CMU (Carnegie Mellon University). https://resources.sei.cmu.edu/asset_files/WhitePaper/2001_019_001_52491.pdf.

Howard, Try E. 2004. "Don't Cache Out Your Case: Prosecuting Child Pornography Possession Laws Based on Images Located in Temporary Internet Files." *Berkeley Technology Law Journal* 19 (4): 1227 –1274. http://www.btlj.org/data/articles2015/vol19/19_4/19-berkeley-tech-l-j-1227-1274.pdf.

Huang, Bunnie. 2016 (Posted on 26 Jul. 2016). "Against the Law: Countering Lawful Abuses of Digital Surveillance." *PubPub*. https://www.pubpub.org/pub/direct-radio-introspection.

I

Illmer, Andreas. 2017 (Posted on 25 Jul. 2017). "China Set to Launch an 'Unhackable' Internet Communication." *BBC*. http://www.bbc.com/news/world-asia-40565722.

International Association of Prosecutors. 2012 (Posted on 11 Jun. 2012). "Global Prosecutors E-Crime Network." *International Association of Prosecutors*. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802f240e.

Information Exchange Network for Mutual Assistance in Criminal Matters and Extradition. 2007. "What is the Law?" *OAS*. https://www.oas.org/juridico/mla/en/can/en_can_mla_what.html.

Information Security Stack Exchange. "Why Do You Need a 4096-bit DSA Key When AES Is Only 256-Bits?" *Information Security Stack Exchange*. http://security.stackexchange.com/questions/59190/why-do-you-need-a-4096-bit-dsa-key-when-aes-is-only-256-bits.

Information Security Stack Exchange. "What Does 'Key with Length of X Bits' Mean?" *Information Security Stack Exchange*. http://security.stackexchange.com/questions/8912/what-does-key-with-length-of-x-bits-mean.

InfoSec Institute. "22 Popular Computer Forensics Tools." *InfoSec Institute*. http://resources.infosecinstitute.com/computer-forensics-tools/.

InfoSecurity Magazine. 2010 (Posted on 20 Aug. 2010). "Do Punishments fit the cybercrime?" *InfoSecurity Magazine*. https://www.infosecurity-magazine.com/magazine-features/do-punishments-fit-the-cybercrime/.

InfoSecurity Magazine. 2011 (Posted on 9 May. 2011). "Cybercrime Knows No Borders." *InfoSecurity Magazine*. http://www.infosecurity-magazine.com/magazine-features/cybercrime-knows-no-borders/.

InfraGard. "About InfraGard." *InfraGard*. https://www.infragard.org/.

Ingber, Stanley. 1987. "The Marketplace of Ideas: A Legitimizing Myth." *Duke Law Journal* 33.

Insa, Fredesvinda. 2007. "The Admissibility of Electronic Evidence in Court (A.E.E.C.): Fighting against High-Tech Crime—Results of a European Study." *Journal of Digital Forensic Practice:* 285-289. http://www.tandfonline.com/doi/pdf/10.1080/15567280701418049.

IADB (Inter-American Development Bank) and OAS (Organization of American States). 2016. *Cybersecurity: Are We Ready in Latin America and the Caribbean?* Washington D.C: IADB. https://publications.iadb.org/bitstream/handle/11319/7449/Cybersecurity-Are-We-Prepared-in-Latin-America-and-the-Caribbean.pdf?sequence=1.

ICMEC (International Centre for Missing and Exploited Children). 2012. *Child Pornography: Model Legislation & Global Review* (7th Edition). Alexandria, Virginia: ICMEC. http://www.icmec.org/wp-content/uploads/2015/10/7th-Edition-EN.pdf.

INTERPOL (International Criminal Police Organization). 2015. *National Cyber Review.* Singapore: *INTERPOL Global Complex for Innovation, Cyber Innovation and Outreach*. https://www.interpol.int/content/download/28038/375648/version/4/file/IGCI-CIO_cyber%20review_projectsheet_2015-03_EN_LR.pdf.

INTERPOL. 2016 (Posted on 22 Jan. 2016). "INTERPOL Backs World Economic Forum Cybercrime Project." *INTERPOL–News*. http://www.interpol.int/News-and-media/News/2016/N2016-010.

INTERPOL. "Command and Coordination Centre—Buenos Aires." *INTERPOL*. http://www.interpol.int/INTERPOL-expertise/Command-Coordination-Centre/Command-and-Coordination-Centre-Buenos-Aires.

INTERPOL. "Cybercrime." *INTERPOL*. http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime.

INTERPOL. "Data Exchange," *INTERPOL*. http://www.interpol.int/INTERPOL-expertise/Data-exchange/I-24-7.

INTERPOL. "Khoo Boon Hui." *INTERPOL*. http://www.interpol.int/About-INTERPOL/Structure-and-governance/KHOO-Boon-Hui.

INTERPOL. "Structure and Governance." *INTERPOL*. http://www.interpol.int/About-INTERPOL/Structure-and-governance/General-Secretariat.

INTERPOL. "The INTERPOL Global Complex for Innovation." *INTERPOL*. http://www.interpol.int/About-INTERPOL/The-INTERPOL-Global-Complex-for-Innovation/About-the-IGCI.

INTERPOL. "World: A Global Presence." *INTERPOL*. http://www.interpol.int/Member-countries/World.

INCB (International Narcotics Control Board). 2001. *Globalization and New Technologies: Challenges to Drug Law Enforcement in the Twenty-first Century.* E/INCB/2001/1. Vienna: INCB. https://www.incb.org/documents/Publications/AnnualReports/AR2001/AR_01_Chapter_I.pdf.

ITU (International Telecommunication Union). 2003. *Geneva Declaration of Principles and the Geneva Plan of Action.* Geneva: ITU. https://www.itu.int/net/wsis/docs/promotional/brochure-dop-poa.pdf.

ITU. 2010. *ITU Toolkit for Cybercrime Legislation (Draft).* Geneva: ITU.http://www.cyberdialogue.ca/wp-content/uploads/2011/03/ITU-Toolkit-for-Cybercrime-Legislation.pdf.

ITU. 2012. "Section II: Model Legislative Text – Cybercrime/e-Crimes." In: HIPCAR, *Cybercrime/e-Crimes: Model Policy Guidelines & Legislative Texts*, 15-28. Geneva: ITU. http://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/reports/wg2/docs/HIPCAR_1-5-B_Model-Policy-Guidelines-and-Legislative-Text_Cybercrime.pdf.

ITU. 2012. "Overview of the Internet of Things." Recommendation ITU-T Y.2060. *Internet of Things Global Standards Initiative*. http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=y.2060.

ITU. 2013. HIPSSA, *Computer Crime and Cybercrime: Southern African Development Community (SADC) Model Law*. Geneva: ITU. http://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/sadc_model_law_cybercrime.pdf.

ITU. 2013. ICBRPAC, *Electronic Crimes: Knowledge-Based Report (Skeleton)*. Geneva: ITU. http://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/ICB4PAC/Documents/FINAL%20DOCUMENTS/cybercrime_skeleton.pdf.

ITU. 2013. "Section II: Model Legislative Text –Electronic Crimes." In: HIPCAR, *Electronic Evidence: Model Policy Guidelines and Legislative Texts*, 13-20. Geneva: ITU. http://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPCAR/Documents/FINAL%20DOCUMENTS/ENGLISH%20DOCS/e-evidence_mpg.pdf.

ITU. 2015. "Annex 3: Cyberwellness country profiles A-Z." In: *Global Cyber Security Index & Cyberwellness Profiles*, 41-515. Geneva: ITU. http://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf.

ITU. "Global Cybersecurity Index." *ITU*. http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx.

ITU. "Global Cybersecurity Agenda (GCA)." *ITU*. http://www.itu.int/en/action/cybersecurity/Pages/gca.aspx.

ITU. "National Cybersecurity Strategies." *ITU*. http://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies.aspx.

Internet & Jurisdiction. 2014."Progress Report 2013-2014." Internet & Jurisdiction: Paris.

Internet Crime Complaint Center & Federal Bureau of Investigation. 2015."Business Email Compromise, Public Service Announcement." *Internet Crime Complaint Center & Federal Bureau of Investigation*. https://www.ic3.gov/media/2015/150122.aspx;

Internet Security Alliance."Cross Cutting Issue #2: How Can We Create Public Private Partnerships that Extended to Action Plans that Work?" *The White House of Barack Obama*. https://obamawhitehouse.archives.gov/files/documents/cyber/ISA%20-%20Hathaway%20public%20private%20partnerships.pdf.

Internet Society. "Brief History of the Internet." *Internet Society*. http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet.

IWF (Internet Watch Foundation). 2008. *IWF Annual Report 2008*. Cambridge: IWF. https://www.iwf.org.uk/assets/media/IWF%20Annual%20Report%202008.pdf.

Internet World Stats. 2017. "World Internet Usage and Population Statistics." *Internet World Stats*. http://www.internetworldstats.com/stats.htm.

J

Jang, Junsik. 2009. "The Current Situation and Countermeasures to Cybercrime and Cyber-Terror in the Republic of Korea." *Resource Material Series* no. 79: 46-56. Tokyo: UNAFEI. http://www.unafei.or.jp/english/pdf/RS_No79/No79_08VE_Jang1.pdf.

Jarrett, H. Marshall, Michael W. Bailie, Ed Hagen and Nathan Judish. 2009. *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* (3rd Edition). Washington D.C. U.S. Department of Justice, Office of Legal Education Executive Office for U.S. Attorneys. http://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf.

Jens Todt, Von. 2007 (Posted on 8 Jan. 2007). Fahnder ueberpruefen erstmals alle deutschen Kreditkarten. *Spiegel Online*. www.spiegel.de/panorama/justiz/0,1518,457844,00.html (in German).

Jingyi, Claire Huang. 2013 (Posted on 21 Dec. 2013). "3 Years' Jail, S$5,000 Fine for Man Who Harassed US Singer." *TodayOnline*. http://www.todayonline.com/singapore/3-years-jail-s5000-fine-man-who-harassed-us-singer?page=1.

Johnson, David R. and David G. Post. 1996 "Law and Borders –The Rise of Law in Cyberspace." *Stanford Law Review* 48: 1367-1402. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=535.

Joyce, Daniel. 2015. "Privacy in the Digital Era: Human Rights Online?" *Melbourne Journal of International Law* 16(1): 270.

Judicial Network & Eurojust. 2014 (Posted 6 May 2014). "Joint Task Force Paper Assistance in International Cooperation in Criminal Matters for Practitioners European." *Press Release, Council of the European Union*. http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressdata/en/jha/104584.pdf.

K

Kaspersky Lab. 2015. *Kaspersky Lab Transparency Principles*. Moscow: Kaspersky Lab. https://cdn.press.kaspersky.com/files/2013/06/Kaspersky-Lab-Transparency-Principles_Q3_2015_final.pdf.

Kaspersky Labs. 2017 (Posted on 13 May 2017). "WannaCry: Are You Safe?" *Kaspersky Labs*. https://blog.kaspersky.com/wannacry-ransomware/16518/.

Kaspersky Labs. 2017 (Posted on 14 May 2017). "Kaspersky Lab's Notice to Customers about the Shadow Brokers' Publication from April 14." *Kaspersky Labs*. https://support.kaspersky.com/shadowbrokers.

Kastrenakes, Jacob. 2015 (Posted on 23 Dec. 2015). "India Temporarily Bans Facebook's Controversial Free Internet Service." *The Verge*. http://www.theverge.com/2015/12/23/10657916/free-basics-internet-org-service-temporary-ban-india.

Keizer, Gregg. 2007 (Posted on 29 Jul. 2007). "FAQ: What We Know (Now) about the FBI's CIPAV Spyware." *Computerworld*. http://www.computerworld.com/article/2542777/security0/faq--what-we-know--now--about-the-fbi-s-cipav-spyware.html.

Kelion, Leo. 2017 (Posted on 1 Aug. 2017). "Dark Web Markets Boom after Alphas Bay and Hansa Busts." *BBC News*. http://www.bbc.com/news/technology-40788266.

Kenneally, Erin. 2005. "Confluence of Digital Evidence and the Law: On the Forensic Soundness of Live-Remote Digital Evidence Collection." *UCLA Journal of Law & Technology* 9(2). http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2145647.

Kerr, Orin S. 2005. "Searches and Seizures in a Digital World." *Harvard Law Review* 119: 531 –585. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=697541.

Khatib, Lina, William H. Dutton and Michael Thelwall. 2012. "Public Diplomacy 2.0: A Case Study of the US Digital Outreach Team." *Middle East Journal* 66(3): 453–472. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1734850.

Kibble, Mary B. 2008. "Fear Mongering, Filters, the Internet and the First Amendment: Why Congress Should Not Pass Legislation Similar to the Deleting Online Predators Act." *Roger Williams University Law Review* 13(2). 497 –529. http://docs.rwu.edu/cgi/viewcontent.cgi?article=1391&context=rwu_LR.

Kiley, Matthew, Tim Shinbara & Marcus Rogers. 2007. "iPod Forensics." *International Journal of Digital Evidence* 4(2).

Kim, Sohee and Meeyoung Cho. 2014 (Posted on 21 Dec. 2014). "South Korea Prosecutors Investigate Data Leak at Nuclear Power Plants." *Reuters*. http://www.reuters.com/article/us-southkorea-nuclear-idUSKBN0JZ05120141221.

King, Rachael. 2012 (Posted on 8 Nov. 2012). "Stuxnet Infected Chevron's IT Network." *Wall Street Journal*. http://blogs.wsj.com/cio/2012/11/08/stuxnet-infected-chevrons-it-network/.

Kinget, Peter. 2014 (Posted on Nov. 2014). "The World Is Analog." *Circuit Cellar*, no. 292. http://www.ee.columbia.edu/~kinget/WhyAnalog/circuitcellar_The_World_Is_Analog_201410.pdf.

Kitchin, Rob and Martin Dodge. 2001. "'Placing' Cyberspace: Why Geography Still Matters." *Information Technology, Education and Society* 1(2): 25-46.

Klip, André. 2013. "Section 4: Concept Paper and Questionnaire." Paper prepared for IAPL's Preparatory Colloquium Section IV for the 20th International Congress of Penal Law on Information Society and Penal Law, "International Criminal Law," Helsinki, 10-12 June. http://www.penal.org/IMG/pdf/Section_IV_EN.pdf.

Kobie, Nicole. 2015 (Posted on 30 Mar. 2015). "Why Electronic Voting Isn't Secure – but May Be Safe Enough." *Guardian*. https://www.theguardian.com/technology/2015/mar/30/why-electronic-voting-is-not-secure.

Kolochenko, Illia. 2016 (Posted on 16 Dec. 2016). "Cybercrime: The Price of Inequality." *Forbes*. http://www.forbes.com/sites/forbestechcouncil/2016/12/19/cybercrime-the-price-of-inequality/2/#1994040176db.

Konnikova, Maria. 2015 (Posted in May 2015). "Virtual Reality Gets Real: The Promises—and Pitfalls—of the Emerging Technology." *The Atlantic*. http://www.theatlantic.com/magazine/archive/2015/10/virtual-reality-gets-real/403225/.

Koons, Stephanie. 2015 (Posted on 21 Jan. 2015). "IST Researchers Examine Role of "White Hat" Hackers in Cyber Warfare." *Penn State: News*. http://news.psu.edu/story/341564/2015/01/21/research/ist-researchers-examine-role-%E2%80%98white-hat%E2%80%99-hackers-cyber-warfare.

Korte, Gregory. 2016 (Posted on 9 Feb. 2016). "Obama Signs Two Executive Orders on Cybersecurity" *USA Today*. http://www.usatoday.com/story/news/politics/2016/02/09/obama-signs-two-executive-orders-cybersecurity/80037452/.

Kottasova, Ivana & Samuel Burke. 2017 (Posted on 27 Mar. 2017). "UK Government Wants Access to WhatsApp Messages." *CNN Tech*. http://money.cnn.com/2017/03/27/technology/whatsapp-encryption-london-attack/index.html.

Kraft, Michael & Edward Marks. 2012. *US Government Counterterrorism: A Guide to Who Does What*. Boca Raton, FL: CRC Press.

Krebs, Albin. 1980 (Posted on 19 Nov. 1980)."Willie Sutton Is Dead at 79." *The New York Times*. http://graphics8.nytimes.com/packages/pdf/books/Willie-Sutton-Obit.pdf.

Krebs, Brian. 2014 (Posted on 14 Jan. 2014). "Target: Names, Emails, Phone Numbers on Up To 70 Million Customers Stolen." *Krebs on Security*. http://krebsonsecurity.com/2014/01/target-names-emails-phone-numbers-on-up-to-70-million-customers-stolen/.

Krebs, Brian. 2015. "Carbanak APT: The Great Bank Robbery." *Kapersky Lab*. http://krebsonsecurity.com/wp-content/uploads/2015/02/Carbanak_APT_eng.pdf.

Krebs, Brian. 2015 (Posted on 15 Jan. 2015)."FBI: Businesses Lost $215M to Email Scams." *Krebs on Security*. http://krebsonsecurity.com/2015/01/fbi-businesses-lost-215m-to-email-scams/.

Krebs, Brian. 2015 (Posted on 15 Feb. 2015). "The Great Bank Heist, or Death by 1,000 Cuts?" *Krebs on Security*. http://krebsonsecurity.com/2015/02/the-great-bank-heist-or-death-by-1000-cuts/.

Kubrick, Stanley, dir. 2001: A Space Odyssey. Writ. Arthur C. Clarke & Stanley Kubrick. Metro Goldwyn-Mayer (MGM), 1968. Film.

Kuchera, Ben. 2008 (23 Oct. 2008). "Dutch Court Imposes Real-World Punishment for Virtual Theft." *Ars Technica*. https://arstechnica.com/gaming/2008/10/dutch-court-imposes-real-world-punishment-for-virtual-theft/.

Kunze, Erin I. 2010. "Sex Trafficking via the Internet: How International Agreements Address The Problem And Fail To Go Far Enough." *Journal of High Technology Law* 10(2): 241 –287. https://www.suffolk.edu/documents/jhtl_publications/kunze.pdf.

Kushner, David. 2013 (Posted on 26 Feb. 2013). "The Real Story of Stuxnet: How Kaspersky Lab Tracked Down the Malware that Stymied Iran's Nuclear-Fuel Enrichment Program." *IEEE Spectrum*. http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet.

L

Laboratory of Cryptography and System Security (CrySyS Lab). 2012 (Posted on 31 May 2012). "sKyWIper (a.k.a. Flame a.k.a. Flamer): A Complex Malware for Targeted Attacks." Budapest University of Technology and Economics. https://www.crysys.hu/skywiper/skywiper.pdf.

Landler, Mark. 2000 (Posted on 21 Oct. 2000). "A Filipino Linked to 'Love Bug' Talks about his License to Hack." *New York Times*. http://www.nytimes.com/2000/10/21/business/a-filipino-linked-to-love-bug-talks-about-his-license-to-hack.html.

Laney Zhang. 2013. "*China: NPC Decision on Network Information Protection.*" Washington, D.C.: Library of Congress, Global Legal Monitor. http://www.loc.gov/law/foreign-news/article/china-npc-decision-on-network-information-protection/.

Lange, Michell C.S. and Kristin M. Nimsger. 2004. *Electronic Evidence and Discovery: What Every Lawyer Should Know.* Chicago: ABA (American Bar Association).

Lasseter, John, dir. 1995. *Toy Story*. Walt Disney Pictures & Pixar Animation Studios. Film.

Law, Jonathan, ed. 2015. "Extradition Treaty." In: *A Dictionary of Law* (8 Ed.). http://www.oxfordreference.com/view/10.1093/acref/9780199664924.001.0001/acref-9780199664924-e-1504?rskey=jCiT5L&result=1642.

Lawrence III, Robert C. 1999. *International Tax and Estate Planning*. 3d ed.

LawTeacher. 2013. "Computer and Cybercrime." *LawTeacher.net*. http://www.lawteacher.net/free-law-essays/technology-law/computer-and-cybercrime.php.

Lee, Dave. 2015 (Posted on 7 Oct. 2015). "How Worried Is Silicon Valley about Safe Harbour?" *BBC News*. http://www.bbc.com/news/technology-34461682.

Lee, Dave. 2017 (Posted on 13 May 2017). "Global Cyber-Attack: How Roots Can be Traced to the US." *BBC News*. http://www.bbc.com/news/technology-39905509.

Lee, Sook-yeon. 2012. "Admissibility and Examination of Digital Evidence: With a Focus on the Criminal Procedure." *Supreme Court Law Journal* 2(2): 11-84. http://library.scourt.go.kr/SCLIB_data/publication/m_531306_v.2-2.pdf.

Legal Information Institute. "Long-Arm Statute." *Cornell University Law School*. https://www.law.cornell.edu/wex/long-arm_statute.

Leigland, Ryan and Axel W. Krings. 2004. "A Formalization of Digital Forensics." *International Journal of Digital Evidence* 3(2). http://people.cis.ksu.edu/~sathya/formalizing-df.pdf.

Lewis, Paul. 2011 (Posted on 2 Mar. 2011). "You're Being Watched: There's One CCTV Camera for Every 32 People in UK." *Guardian*. https://www.theguardian.com/uk/2011/mar/02/cctv-cameras-watching-surveillance.

Lewontin, Max. 2016 (Posted on 8 Feb. 2016). "Why Defeat in India Leaves an Uncertain Path for Facebook's 'Free Basics'" *The Christian Science Monitor*. http://www.csmonitor.com/Technology/2016/0208/Why-defeat-in-India-leaves-an-uncertain-path-for-Facebook-s-Free-Basics.

Leyden, John. 2005 (Posted on 25 Jul. 2005). "UK War Driver Fined £500." *The Register*. http://www.theregister.co.uk/2005/07/25/uk_war_driver_fined/.

Leyden, John. 2008. "FBI Sought Approval to Use Spyware against Terror Suspects." *The Register*. http://www.theregister.co.uk/2008/02/08/fbi_spyware_ploy_app/.

Library of Congress. 2014. *Full Report of European Union: ECJ Invalidates Data Retention Directive*. Washington D.C.: Library of Congress. http://www.loc.gov/law/help/eu-data-retention-directive/eu-data-retention-directive.pdf.

Litvinova, Dari. 2015 (Posted on 1 Sep. 2015). "Russia's New Personal Data Law Will Be Hard to Implement, Experts Say." *The Moscow Times*. http://www.themoscowtimes.com/news/article/russias-new-personal-data-law-will-be-hard-to-implement-experts-say/529195.html.

Lloyd, Ian J.2014. *Information Technology Law* (7th Edition). London: Oxford University Press.

Luiijf, Eric, Kim Besseling and Patrick De Graaf. 2013. "Nineteen National Cyber Security Strategies." *International Journal of Critical Infrastructures* 9 (1-2): 3 –31.

Lynch, James P. 1987. "Routine Activity and Victimization at Work." *Journal of Quantitative Criminology* 3 (4):283-300.

M

MacAskill, Ewen. 2016 (Posted on 19 Nov. 2016). "'Extreme Surveillance' Becomes UK Law with Barely a Whimper." *Guardian*. https://www.theguardian.com/world/2016/nov/19/extreme-surveillance-becomes-uk-law-with-barely-a-whimper.

Macovei, Monica. 2004. *Freedom of Expression: A guide to the Implementation of Article 10 of the European Convention on Human Rights* (2nd Edition). Human Rights Handbooks, No 2. Strasbourg: Council of Europe. http://www.echr.coe.int/LibraryDocs/DG2/HRHAND/DG2-EN-HRHAND-02(2004).pdf.

Malaga. 2008. "Requirements for the Admissibility in Court of Digital Evidence." in: *Syllabus to the European Certificate on Cybercrime and E-Evidence*.

Malby, Steven, Tejal Jesrani, Tania Bañuelos, Anika Holterhof & Magdalena Hahn. 2011. *Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children*. Vienna: UNODC. http://www.unodc.org/documents/organized-crime/cybercrime/Study_on_the_Effects.pdf.

Malmström, Cecilia. 2012. "Public-private Cooperation in the Fight against Cybercrime." Speech made at the EU Cybersecurity & Digital Crimes Forum, Brussels, 31 May. http://europa.eu/rapid/press-release_SPEECH-12-409_en.pdf.

MalwareTech. 2017 (Posted on 13 May 2017). "How to Accidentally Stop a Global Cyber Attacks." *MalwareTech Blog*. https://www.malwaretech.com/2017/05/how-to-accidentally-stop-a-global-cyber-attacks.html.

Manes, Gavin W., Elizabeth Downing, Lance Watson and Christopher Thrutchley. 2007. "New Federal Rules and Digital Evidence." Paper Prepared for the ADFSL (Association of Digital Forensics, Security and Law) Conference, "Digital Forensics, Security and Law," Alexandria, 18-20 Apr. http://proceedings.adfsl.org/index.php/CDFSL/article/viewFile/12/12.

Marcella Jr., Albert and Doug Menendez. 2007. *Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes* (2nd Edition). Boca Raton: Auerbach Publications.

Marino, Catalina Botero (Special Rapporteur for Freedom of Expression Inter-American Commission on Human Rights). 2013. *Freedom of Expression and the Internet.* OEA/Ser.L/V/ II CIDH/RELE/INF.11/13. Washington D.C.: OAS. http://www.oas.org/en/iachr/expression/docs/reports/2014_04_08_Internet_ENG%20_WEB.pdf.

Marlinspike, Moxie. 2013 (Posted on 13 Jun. 2013). "Why 'I Have Nothing to Hide' Is the Wrong Way to Think about Surveillance." Wired. https://www.wired.com/2013/06/why-i-have-nothing-to-hide-is-the-wrong-way-to-think-about-surveillance/.

Marsh, James R. 2011. "Masha's Law: A Federal Civil Remedy for Child Pornography Victims." *Syracuse Law Review* 61(3): 459 –497. http://heinonline.org/HOL/Page?handle=hein.journals/syrlr61&div=25&g_sent=1&collection=journals.

Martinez, Edecio and Albert Gonzalez. 2010 (Posted on 26 Mar. 2010). "SoupNazi" Credit Card Hacker, Gets 20 Years." *CBS News.* http://www.cbsnews.com/news/albert-gonzalez-soupnazi-credit-card-hacker-gets-20-years/.

Mas, Ignacio & Dan Radcliffe. 2011. "Mobile Payments Go Viral M-PESA in Kenya." *Capco Journal of Financial Transformation* 32.

Mason, Stephen, ed. 2007. *Electronic Evidence: Discovery, Disclosure and Admissibility.* London: LexisNexis (U.K.)–Butterworths.

Mathai, Anahita. 2015 (Posted on 12 Mar. 2015). "The Budapest Convention and Cyber Cooperation." *ORF Cyber Monitor.*

Maurer, Ueli. 1997. "Information-Theoretically Secure Secret-Key Agreement by NOT Authenticated Public Discussion," in: EUROCRYPT'97 Proceedings of the 16th annual international conference on Theory and application of cryptographic techniques. ftp://ftp.inf.ethz.ch/pub/crypto/publications/Maurer97.pdf.

McAFee. 2016. "Infographic: McAfee Labs Threats Report." *McAFee.* https://www.mcafee.com/us/resources/misc/infographic-threats-report-mar-2016.pdf.

McAfee & CSIS. 2014. "Net Losses: Estimating the Global Cost of Cybercrime." *CSIS.* http://csis.org/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf.

McBath, J. Elizabeth. 2012. "Trashing Our System of Justice? Overturning Jury Verdicts Where Evidence Is Found in the Computer's Cache." *American Journal of Criminal Law* 39 (3): 381-424.

McCormack, Wayne. 2014. "U.S. Judicial Independence: Victim in the "War on Terror"." *Washington and Lee Law Review* 71(1): 305 –402. http://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?article=4374&context=wlulr.

McCormick, Charles T. et al. 1992. *McCormick on Evidence*, 4th ed. St. Paul, MN: West Pub.

McCullagh, Declan. 2005 (Posted on 28 Nov. 2005). "Fuzzy Logic Behind Bush's Cybercrime Treaty." *CNET*. http://www.cnet.com/news/fuzzy-logic-behind-bushs-cybercrime-treaty/.

McCullagh, Declan. 2006 (Posted on 8 Aug. 2006). "Senate Ratifies Controversial Cybercrime Treaty." *CNET*. http://www.cnet.com/news/senate-ratifies-controversial-cybercrime-treaty/.

McCullagh, Declan. 2007 (Posted on 18 Jul. 2007). "FBI Remotely Installs Spyware to Trace Bomb Threat." *CNET*. http://www.cnet.com/news/fbi-remotely-installs-spyware-to-trace-bomb-threat/.

McCurry, Justin. 2014 (Posted on 23 Dec. 2014). "South Korean Nuclear Operator Hacked Amid Cyber-Attack Fears." *The Guardian*. http://www.theguardian.com/world/2014/dec/22/south-korea-nuclear-power-cyber-attack-hack.

McGath, Gary 2016. "Net Neutrality Kills Free Internet - Is Internet Access a Basic Human Right?" Atlanta: FEE (Foundation for Economic Education). https://fee.org/articles/net-neutrality-kills-free-internet/.

McKinsey & Company. 2016. "How Blockchains Could Change the World." *McKinsey & Company*. http://www.mckinsey.com/industries/high-tech/our-insights/how-blockchains-could-change-the-world.

Melander, Sakari. 2013. "Ultima Ratio in European Criminal Law." *Oñate Socio-Legal Series* 3(1): 42–61. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2200871.

Mendel, Toby. 2000. "Freedom of Information as an Internationally Protected Human Right." In: *American Civil Liberties Union International Civil Liberties Report*. Los Angeles: ACLU (American Civil Liberties Union). https://www.article19.org/data/files/pdfs/publications/foi-as-an-international-right.pdf.

Menn, Joseph. 2015 (Posted on 29 May 2015). "Exclusive: US Tried Stuxnet-Style Campaign Against North Korea but Failed—Sources." *Reuters*. http://www.reuters.com/article/us-usa-northkorea-stuxnet-idUSKBN0OE2DM20150529.

Metz, Cade. 2016 (Posted on 5 Apr. 2016). "Forget Apple vs. the FBI: WhatsApp Just Switched on Encryption for a Billion People." *Wired*. http://www.wired.com/2016/04/forget-apple-vs-fbi-whatsapp-just-switched-encryption-billion-people/.

Meyers, Matthew and Marc Rogers. 2004. "Computer Forensics: The Need for Standardization and Certification." *International Journal of Digital Evidence* 3(2) https://utica.edu/academic/institutes/ecii/publications/articles/A0B7F51C-D8F9-A0D0-7F387126198F12F6.pdf.

Microsoft. 2008. *Case Study: Forefront Helping to Protect Australia's Borders from Illegal Immigration, Drug Smuggling and Other Security Threats.* Redmond: Microsoft.

Microsoft. 2015. *Microsoft Security Intelligence Report* Vol. 19 (January –June 2015). Redmond: Microsoft. http://download.microsoft.com/download/4/4/C/44CDEF0E-7924-4787-A56A-16261691ACE3/Microsoft_Security_Intelligence_Report_Volume_19_English.pdf.

Microsoft.2016. *Microsoft Security Intelligence Report* Vol. 21. *Microsoft.* https://blogs.microsoft.com/microsoftsecure/2016/12/14/microsoft-security-intelligence-report-volume-21-is-now-available/.

Microsoft. 2017 (Posted on 14 Mar. 2017). Security Bulletin MS17-010. *Microsoft.* https://technet.microsoft.com/en-us/library/security/ms17-010.aspx.

Microsoft Security Response Center. 2017 (Posted on 12 May 2017). "Customer Guidance for WannaCrypt Attacks." *Microsoft.* https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/.

Miethe, Terance D. and Robert F. Meier. 1990. "Criminal Opportunity and Victimization rates: A Structural-choice Theory of Criminal Victimization." *Journal of Research in Crime and Delinquency* 27:243-66.

Milanovic, Marko. 2015. "Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age." *Harvard International Law Journal* 56(1): 81 to 146. http://www.harvardilj.org/wp-content/uploads/561Milanovic.pdf.

Miller, Joe. 2014 (Posted on 19 Sep. 2014). "Google and Apple to introduce Default Encryption." *BBC.* http://www.bbc.com/news/technology-29276955.

Miquelon-Weismann, Miriam F. 2005. "The Convention on Cybercrime: A Harmonized Implementation of International Penal Law: What Prospects for Procedural Due Process." *John Marshall Journal of Computer and Information Law* 23(2): 329 –361. http://repository.jmls.edu/cgi/viewcontent.cgi?article=1057&context=jitpl.

Mitchell, William J. 1995. *City of Bits: Space, Place and the Infobahn.* Cambridge: MIT Press. https://mitpress.mit.edu/sites/default/files/9780262133098.pdf.

Moir, Iain, George R. S. Weir. 2008. "Identity Theft: A Study in Contact Centres." Paper presented at the 4th International Conference on Global E-Security, London, 23-28 Jun. http://www.cis.strath.ac.uk/cis/research/publications/papers/strath_cis_publication_2243.pdf.

Moitra, Soumyo D. 2004. "Cybercrime: Towards an Assessment of its Nature and Impact." *International Journal of Comparative and Applied Criminal Justice* 28 (2): 105 –120.

Molina, Fernando. 2011. "A Comparison Between Continental European and Anglo-American Approaches to Overcriminalization and Some Remarks on How to Deal with It." *New Criminal Law Review* 14 (1): 123–138.

Moore, Robert. 2004. "To View or Not to View: Examining the Plain View Doctrine and Digital Evidence." *American Journal of Criminal Justice* 29(1): page 57 –73.

Morris, Jr., John B. 2011. *Hearing on "Data Retention as a Tool For Investigating Internet Child Pornography And Other Internet Crimes.* Washington D.C.: CDT (Center for Democracy & Technology). https://cdt.org/files/pdfs/20110124_morris_DataRetention_testi.pdf.

Mott, Nathaniel. 2016 (15 Jun. 2016). "Take That, FBI: Apple Goes All in on Encryption." *Guardian*. https://www.theguardian.com/technology/2016/jun/15/apple-fbi-file-encryption-wwdc.

Mullen, Paul. Michele Pathé & Rosemary Purcell. "Cyberstalking." *Stalking Risk Profile*. https://www.stalkingriskprofile.com/victim-support/impact-of-stalking-on-victims.

Munro, Susan and Lin Yang. 2015. "China Promulgates the Ninth Amendment to the PRC criminal law." Washington, D.C.: Steptoe & Johnson LLP. http://www.steptoe.com/publications-10742.html.

N

National Center for Victims of Crime. "Stalking Technology Outpaces State Laws." *National Center for Victims of Crime*. https://victimsofcrime.org/docs/src/stalking-technology-outpaces-state-laws17A308005D0C.pdf?sfvrsn=2.

National Conference of State Legislature. "National Conference of State Legislature." *National Conference of State Legislature*. http://www.ncsl.org/.

NCFTA (National Cyber-Forensics and Training Alliance). "Who We Are." *NCFTA*. http://www.ncfta.net/.

NCFTA. 2016 (Posted on 8 Jan. 2016). "NCFTA in the News: The National Cyber-Forensics and Training Alliance to Open New Offices in Los Angeles and New York." *NCTFA*. https://www.ncfta.net/Home/News.

NCFTA. 2016 (Posted on 18 Jul. 2016). "NCFTA in the News: International Alliance Against Counterfeiting." *NCTFA*. https://www.ncfta.net/Home/News.

NCFTA. "CyFin." *NCFTA*. http://www.ncfta.net/Home/Cyfin.

NCFTA. "BCP." *NCFTA*. http://www.ncfta.net/Home/BCP.

NCFTA. "MCT." *NCFTA*. http://www.ncfta.net/Home/Malware.

National Institute of Justice (NIJ). "Digital Evidence and Forensics." *U.S. Department of Justice*. http://www.nij.gov/topics/forensics/evidence/digital/Pages/welcome.aspx.

National Institute of Standards and Technology (NIST). "Computer Forensics Tool Testing Project." *NIST*. http://www.cftt.nist.gov.

NIST. 2016 (Posted on 4 Oct. 2016). "'Security Fatigue' Can Cause Computer Users to Feel Hopeless and Act Recklessly." *NIST*. https://www.nist.gov/news-events/news/2016/10/security-fatigue-can-cause-computer-users-feel-hopeless-and-act-recklessly.

National White Collar Crime Center. 2011. *Criminal Use of Social Media (2011)*. Fairmont: National White Collar Crime Center. http://www.iacpsocialmedia.org/Portals/1/documents/External/NW3CArticle.pdf.

NDTV Correspondent. 2015 (Posted on 28 May. 2015). "Gaana.com Confirms Its User Database Was Hacked." *Gadgets360*. http://gadgets.ndtv.com/internet/news/gaanacom-allegedly-hacked-details-of-all-users-exposed-697111.

Neumayer, Eric. 2007. "Qualified Ratification: Explaining Reservations to International Human Rights Treaties." *Journal of Legal Studies* 36(2): 397 –430. http://eprints.lse.ac.uk/3051/1/Qualified_ratification_(LSERO).pdf.

News Report. 2006 (Posted 4 Aug. 2006). "CSIA Applauds Ratification of Cybercrime Treaty." *GT (Government Technology)*. http://www.govtech.com/security/CSIA-Applauds-Ratification-of-Cybercrime-Treaty.html.

Nicoll, Chris. 2003. "Concealing and Revealing Identity on the Internet." In: *Digital Anonymity and the Law* edited by Chris Nicoll, J. E. J. Prins and Miriam J. M. van Dellen, 99-120. The Hague: T.M.C. Asser Press.

Nijboer, Johannes F. 2013. "Section 3: Concept Paper and Questionnaire." Paper prepared for IAPL's Preparatory Colloquium Section III for the 20th International Congress of Penal Law on Information Society and Penal Law, "Criminal Procedure," Antalya, 23-26 September. http://www.penal.org/IMG/pdf/Section_III_EN.pdf.

Nolan, Richard, Colin O'Sullivan, Jake Branson and Cal Waits. 2005. *First Responders Guide to Computer Forensics*. Arlington: SEI (Software Engineering Institute). http://www.sei.cmu.edu/reports/05hb001.pdf.

NATO. 2011. "G8 Declaration Renewed Commitment for Freedom And Democracy." G8 Summit of Deauville, (26–27 May 2011). http://www.nato.int/nato_static/assets/pdf/pdf_2011_05/20110926_110526-G8-Summit-Deauville.pdf.

NATO (North Atlantic Treaty Organization). 2016. "Warsaw Summit Communiqué, Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Warsaw 8–9 July 2016: Press Release (2016) 100." http://www.nato.int/cps/en/natohq/official_texts_133169.htm.

NTT Innovation Institute, Inc. 2015. *2015 Global Threat Intelligence Report –Executive Summary.* East Palo Alto: NTT Innovation Institute, Inc. http://www.nttcomsecurity.com/en/uploads/files/US_GTIR_Executive_Summary_Public_Approved_v8.pdf.

Nugent, John. "Cyber Security Outlook." In: *RISKMAP REPORT 2016.* Washington D.C.: Control Risks, 22-23. https://www.controlrisks.com/webcasts/studio/flipping-book/riskmap_report_2016/files/assets/common/downloads/RISKMAP%202016%20REPORT.pdf.

Nussbaum, Ania. 2015 (Posted on 18 Jun. 2015). "Russia's Data Law Will Hurt Its Economy –Think Tank." *The Wall Street Journal: Digits.* http://blogs.wsj.com/digits/2015/06/18/russias-data-law-will-hurt-its-economy-think-tank/.

O

Obama, Barack. 2009 (Posted on 29 May. 2009). "Remarks by the President on Securing Our Nation's Cyber Infrastructure." *The White House –Office of the Press Secretary*. https://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure.

OECD (Office of Economic Cooperation and Development). 2013. Guidelines for the Security of Information Systems and Network. Paris: OECD. https://www.oecd.org/sti/ieconomy/privacy-guidelines.htm.

Office of the Privacy Commissioner of Canada. 2015. *Fact Sheet on the Digital Privacy Act.* Gatineau, Quebec. Office of the Privacy Commissioner of Canada. https://www.priv.gc.ca/resource/fs-fi/02_05_d_63_s4_e.pdf.

Official Microsoft Blog. "Botnets." *Microsoft*. https://blogs.microsoft.com/blog/tag/botnets/#sm.000013htf1t8ngf0zuycn3473chdh.

O'Harrow Jr., Robert. 2005. *No Place to Hide*. New York: Free Press.

Oh, Gi-du.2013. "Statement of Defendant and Authentication of Electronic Documents." *Supreme Court Law Journal* 3(2): 71-114. http://library.scourt.go.kr/SCLIB_data/publication/m_531306_v.3-2.pdf.

Ollmann, Gunter. 2007. *The Phishing Guide: Understanding & Preventing Phishing Attacks*. New York: IBM (IBM Global Technology Services). http://www-935.ibm.com/services/us/iss/pdf/phishing-guide-wp.pdf.

Ondieki, Elvis. 2016 (Posted on 8 May 2016). "M-Pesa Transactions Rise to Sh15bn Daily after Systems Upgrade." http://www.nation.co.ke/news/MPesa-transactions-rise-to-Sh15bn-after-systems-upgrade/1056-3194774-llu8yjz/index.htmln.

Open Rights Group. 2015. *Data retention in the EU following the CJEU ruling – updated April 2015.* London: Open Rights Group. https://www.openrightsgroup.org/assets/files/legal/Data_Retention_status_table_updated_April_2015_uploaded_finalwithadditions.pdf.

OAS. "G8 – 24/7 Network." Organization of American States (OAS). *OAS*. http://www.oas.org/juridico/english/cyber_g8.htm.

OAS (Organization of American States). 2000. Final Report of the Second Meeting of Government Experts on Cyber Crime. *OAS*. http://www.oas.org/juridico/english/cybGE_IIrep.pdf

OAS. "Who We Are." *OAS*. http://www.oas.org/en/about/who_we_are.asp.

OAS. "Cyber Security," *OAS*. https://www.sites.oas.org/cyber/en/Pages/default.aspx.

OAS. "Welcome," Inter-American Cooperation Portal on Cyber-Crime. *OAS*. http://www.oas.org/juridico/english/cyber.htm

OAS. 2006. *Questionnaire Related to the Recommendations from the Fourth Meeting of Governmental Experts on Cyber-Crime*. Washington D.C.: OAS. http://www.oas.org/juridico/english/cybGE_IVquest.doc.

OAS. 2007. *The G8 24/7 Network of Contact Points: Protocol Statement*. Washington D.C.: OAS. http://www.oas.org/juridico/english/cyb_pry_G8_network.pdf.

OAS. 2011. "Freedom of Expression Rapporteurs Issue Joint Declaration Concerning the Internet." *OAS*. http://www.oas.org/en/iachr/expression/showarticle.asp?artID=848.

OAS. 2016. "Best Practices for Establishing a National CSIRT." *OAS*. https://www.sites.oas.org/cyber/Documents/2016%20-%20Best%20Practices%20CSIRT.pdf.

OECS (Organization for Eastern Caribbean States). 2011. *Electronic Crimes Bill (Fourth Draft).* Castries: OECS. http://www.oecs.org/publications/e-government-for-regional-integration-project/oecs-harmonized-e-government-legislation/575-electronic-crimes-bill-ags-09-10-11/file.

Osgood, D. Wayne, Janet K. Wilson, Patrick M. O'Malley, Jerald G. Bachman and Lloyd D. Johnston. 1996. "Routine Activities and Individual Deviant Behavior." *American Sociological Review.* 61 (4): 635-55.

Osiander, Andreas. 2011. "Sovereignty, International Relations, and the Westphalian Myth." *International Organization Vol. 55.*

Otake, Tomoko. 2015 (Posted on 1 Jun 2015). "1.25 million Affected by Japan Pension Service Hack". *Japan Times.* http://www.japantimes.co.jp/news/2015/06/01/national/crime-legal/japan-pension-system-hacked-1-25-million-cases-personal-data-leaked/#.VvVfpNIrKUk.

P

Paganini, Pierluigi. 2015 (Posted on 18 Mar. 2015). "South Korea—Hacker Requests Money for Data on Nuclear Plants." *Security Affairs.* http://securityaffairs.co/wordpress/35013/cyber-crime/hacker-south-korean-nuclear-plants.html.

Palatino, Mong. 2014 (Posted on 24 Mar. 2014). "Singapore Criminalizes Cyber Bullying and Stalking." *Diplomat.* http://thediplomat.com/2014/03/singapore-criminalizes-cyber-bullying-and-stalking/.

Pandey, Avaneesh. 2016 (Posted on 28 Feb. 2016). "Energy-Efficient 'Biocomputer' Provides Viable Alternative to Quantum Computers." *IBT.* http://www.ibtimes.com/energy-efficient-biocomputer-provides-viable-alternative-quantum-computers-2326448.

Parliamentary Office of Science and Technology (POST). 2015 (Posted on 9 Mar. 2015). "The Darknet and Online Anonymity." UK Houses of Parliament, No. 488. http://researchbriefings.parliament.uk/ResearchBriefing/Summary/POST-PN-488.

Parsons, Mark and Peter Colegate. 2015 (Posted on 12 Feb. 2015). "2015: The Turning Point for Data Privacy Regulation in Asia?" In: *Data Protection & Law Policy (January 2015). Hogan Lovells Chronical of Data Protection.* http://www.hldataprotection.com/2015/02/articles/international-eu-privacy/2015-the-turning-point-for-data-privacy-regulation-in-asia/.

Patel, Ahmed and Séamus Ó Ciardhuáin. 2000. "The Impact of Forensic Computing on Telecommunication." *IEEE Communications Magazine* 38 (11): 64 –67.

Paxson, Vern. 2001. "An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks." *ACM SIGCOMM Computer Communication Review* 31(3): 38 –47. http://www.icir.org/vern/papers/reflectors.CCR.01.pdf.

PC World. 2016 (Posted on 20 Apr. 2016). "SpyEye Botnet Kit Developer Sentenced to Long Jail Term." *PC World.* http://www.pcworld.com/article/3059557/spyeye-botnet-kit-developer-sentenced-to-long-jail-term.html.

Pearson, Sarah Hinchliff. 2009 (Posted on April 17 2009). "The Dynamic Balance between Free Speech and Privacy Interests." *Stanford Law School Blog.* http://cyberlaw.stanford.edu/blog/2009/04/dynamic-balance-between-free-speech-and-privacy-interests.

Perlroth, Nicole. 2017 (Posted on 6 Jul. 2017). "Hackers Are Targeting Nuclear Facilities, Homeland Security Dept. and F.B.I. Say." *New York Times.* https://www.nytimes.com/2017/07/06/technology/nuclear-plant-hack-report.html?mcubz=0.

Persak, Nina. 2007. *Criminalizing Harmful Conduct: The Harm Principle, its Limits and Continental Counterparts.* Berlin-Heidelberg: Springer.

Peterson, Andrea. 2014 (Posted on 18 Dec. 2014). "The Sony Pictures Hack, Explained." *Washington Post.* https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/.

Philippe, Xavier. 2006. "The Principles of Universal Jurisdiction and Complementarity: How Do the Two Principles Intermesh?" *International Review of the Red Cross* 88, no. 862. https://www.icrc.org/eng/assets/files/other/irrc_862_philippe.pdf.

Phpsecurity. "Injection Attacks." *Phpsecurity.* http://phpsecurity.readthedocs.io/en/latest/Injection-Attacks.html.

PM. 2016 (Posted on 22 Jul. 2016). "Could a New Case Stop Your Phone from Being Hacked?" *BBC News.* http://www.bbc.co.uk/programmes/p0428n3p.

Popa, Bogdan. 2007 (Posted on 19 Jul. 2007). "FBI Fights against Terrorists with Computer Viruses." *Softpedia.* http://news.softpedia.com/news/FBI-Fights-Against-Terrorists-With-Computer-Viruses-60417.shtml.

Porcedda, Maria Grazia. 2012. "Data Protection and the Prevention of Cybercrime: The EU as an Area of Security?" EUI Working Papers, EUI (European University Institute), Florence. http://cadmus.eui.eu/bitstream/handle/1814/23296/LAW-2012-25.pdf?sequence=1&isAllowed=y.

Poulsen, Kevin. 2007 (Posted on 18 Jul. 2007). "FBI's Secret Spyware Tracks down Teen Who Makes Bomb Threats." *ABC News.* http://abcnews.go.com/Technology/story?id=3389624.

Privacy International. "What Is Data Protection?" *Privacy International.* https://www.privacyinternational.org/node/44.

Putnam, Tonya L. and David D. Elliott. 2001. "Chapter 2: International Responses to Cyber Crime." In: *The Transnational Dimension of Cyber Crime and Terrorism* edited by Abraham D. Sofaer and Seymour E. Goodman, 35 –67. Stanford: Hoover Institution Press.http://www.hoover.org/sites/default/files/uploads/documents/0817999825_35.pdf.

PwC (PricewaterhouseCoopers). 2014. *Financial Services Sector Analysis of PwC's 2014 Global Economic Crime Survey: Threats to the Financial Services Sector.* Washington D.C.: PwC. https://www.pwc.com/gx/en/financial-services/publications/assets/pwc-gecs-2014-threats-to-the-financial-services-sector.pdf.

PWC. 2014. *PWC's 2014 Global Economic Crime Survey: Economic Crime, A Threat to Business Globally*. https://www.pwc.at/publikationen/global-economic-crime-survey-2014.pdf.

Q

Quarmby, Katharine. 2014 (Posted on 13 Aug. 2014). "How the Law Is Standing Up to Cyberstalking." *Newsweek*. http://www.newsweek.com/2014/08/22/how-law-standing-cyberstalking-264251.html.

Quismundo, Tarra. 2014 (11 Oct. 2014). "DOJ, NU Join Forces against Cybercrime." *Philippine Daily Inquirer*. http://technology.inquirer.net/38998/doj-nu-join-forces-against-cybercrime.

R

Raghavan, A.R. and Latha Parthiban. 2014. "The Effect of Cybercrime on a Bank's Finances." *International Journal of Current Research and Academic Review* 2(2): 173 to 174. http://www.ijcrar.com/vol-2-2/A.R.%20Raghavan%20and%20Latha%20Parthiban.pdf.

Rajan, Nandagopal. 2016 (Posted on 12 Apr. 2016). "WhatsApp Is Not Breaking Indian Laws with 256-Bit Encryption, for Now." *Indian Express*. http://indianexpress.com/article/technology/social/whatsapp-end-to-end-encryption-not-illegal-in-india/.

Rath, David. 2016 (Posted on 11 Oct. 2016). "Legislating Cybersecurity: Lawmakers Recognize Their Responsibility with Cyberthreats." *Government Technology.* http://www.govtech.com/security/Legislating-Cybersecurity-Lawmakers-Recognize-Their-Responsibility-with-Cyberthreats.html.

Rayman, Noah. 2014 (Posted on 7 Aug. 2014). "The World's Top 5 Cybercrime Hotspots." *Time*. http://time.com/3087768/the-worlds-5-cybercrime-hotspots/.

Rehberg, Megan and Susan W. Brenner. 2010. "'Kiddie Crime?' The Utility of Criminal Law in Controlling Cyberbullying." *First Amendment Law Review.* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1537873.

Reith, Mark, Clint Carr, Gregg Gunsch. 2002. "An Examination of Digital Forensic Models." *International Journal of Digital Evidence* 1(3). https://www.utica.edu/academic/institutes/ecii/publications/articles/A04A40DC-A6F6-F2C1-98F94F16AF57232D.pdf.

Repeta, Lawrence. 1999. *Local Government Disclosure Systems in Japan*. Seattle: The National Bureau of Asian Research. http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN026259.pdf.

Roberts, Alasdair S. 2001. "Structural Pluralism and the Right to Information." *University of Toronto Law Journal* 51(3): 243-271. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1305423.

Rosenblum, Paula. 2014 (Posted on 17 Mar. 2014). "In Wake of Target Data Breach, Cash Becoming King Again." *Forbes*. http://www.forbes.com/sites/paularosenblum/2014/03/17/in-wake-of-target-data-breach-cash-becoming-king-again/.

Rossignol, Joe. 2015 (Posted on 24 Sep 2015). "Apple Lists Top 25 Apps Compromised by XcodeGhost Malware." *MacRumors –Newsletter*. http://www.macrumors.com/2015/09/24/xcodeghost-top-25- apps-apple-list/.

RT. 2015 (Posted on 22 May. 2015). "Yemeni Group Hacks 3,000 Saudi Govt Computers to Reveal Top Secret Docs – Report." *RT*. https://www.rt.com/news/261073-yemen-cyber-hack-saudi/.

Rudd, Amber. 2017 (Posted on 25. Mar. 2017). "Social Media Firms Must Join the War on Terror." *Telegraph*. http://www.telegraph.co.uk/news/2017/03/25/social-media-firms-must-join-war-terror/.

Ruibin, Gon, Tony Kai Yun Chan and Mathias Gaertner. 2005. "Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework." *International Journal of Digital Evidence* 4(1). http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.81.4278&rep=rep1&type=pdf.

Russon, Mary-Ann. 2016 (Posted on 7 Apr. 2016). "Quantum Cryptography Breakthrough: 'Unbreakable Security' Possible Using Pulse Laser Seeding." *International Business Times*. http://www.ibtimes.co.uk/quantum-cryptography-breakthrough-unbreakable-security-possible-using-pulse-laser-seeding-1553721.

S

Sacco, Lisa N. 2015. "The Violence Against Women Act: Overview, Legislation, and Federal Funding." *U.S. Congressional Research Service*. https://www.fas.org/sgp/crs/misc/R42499.pdf.

Salkever, Alex. 2001 (Posted on 27 Nov. 2001). "A Dark Side to the FBI's Magic Lantern." *Bloomberg*. http://www.bloomberg.com/news/articles/2001-11-26/a-dark-side-to-the-fbis-magic-lantern.

Salvador, Joseph. 2015. "Dismantling the Internet Mafia: RICO's Applicability to Cyber Crime." *Rutgers Computer & Technology Law Journal* 41(2): 268 –297.

Sampson, Robert J. and John D. Woodredge. 1987. "Linking the Micro- and Macro-level Dimensions of Lifestyle-routine Activity and Opportunity Models of Predatory Victimization." *Journal of Quantitative Criminology* 3 (4): 371-93.

Sanger, David E. & Nicole Perlroth. 2014 (Posted on 17 Dec. 2014). "US Said to Find North Korea Ordered Cyberattack on Sony." *New York Times.* http://www.nytimes.com/2014/12/18/world/asia/us-links-north-korea-to-sony-hacking.html?_r=1.

SANS Institute."SANS Courses." SANS. https://uk.sans.org/courses.

Schjolberg, Stein. 2003. *The Legal Framework – Unauthorized Access to Computer Systems: Penal Legislation in 44 Countries.* Moss District Court, Norway.

Schmidt, Michael S. 2012 (Posted on 2 Aug. 2012). "Cybersecurity Bill Is Blocked in Senate by G.O.P. Filibuster." *New York Times.* http://www.nytimes.com/2012/08/03/us/politics/cybersecurity-bill-blocked-by-gop-filibuster.html?_r=0.

Schuba, Christoph L., Ivan V. Krsul, Markus G. Kuhn, Eugene H. Spafford and Aurobindo Sundaram, Diego Zamboni. 1996. "Analysis of a Denial of Service Attack on TCP." *Computer Science Technical Reports.* Paper 1327. http://docs.lib.purdue.edu/cgi/viewcontent.cgi?article=2326&context=cstech.

Science News. 2013 (Posted on 22 May 2013). "Big Data, for Better or Worse: 90% of World's Data Generated Over Last Two Years." *Science Daily.* https://www.sciencedaily.com/releases/2013/05/130522085217.htm.

Scott, Mark. 2015 (Posted on 12 Jan. 2015). "British Prime Minister Suggests Banning Some Online Messaging Apps." *New York Times: Bits.* http://bits.blogs.nytimes.com/2015/01/12/british-prime-minister-suggests-banning-some-online-messaging-apps/?_r=0.

Secretary of Defense Ash Carter & Chairman of the Joint Chiefs of Staff General Joseph F. Dunford. 2016 (Posted on 29 Feb. 2016). Dept. of Defense Press Briefing. *Pentagon Briefing Room.* http://www.defense.gov/News/News-Transcripts/Transcript-View/Article/682341/department-of-defense-press-briefing-by-secretary-carter-and-gen-dunford-in-the

Selyukh, Alina and Camila Domonoske. 2016 (Posted on 17 Feb. 2016). "Apple, The FBI and iPhone Encryption: A Look at what's at stake." *NPR.* http://www.npr.org/sections/thetwo-way/2016/02/17/467096705/apple-the-fbi-and-iphone-encryption-a-look-at-whats-at-stake.

Sembhi, Sarb. 2009 (Posted on Feb. 2009). "How to Defend against Data Integrity Attacks." *Computer Weekly.* http://www.computerweekly.com/opinion/How-to-defend-against-data-integrity-attacks.

Sen, Jaydip. 2013. "Chapter 1: Security and Privacy Issues in Cloud Computing." In: *Architectures and Protocols for Secure Information Technology Infrastructures* edited by Antonio Ruiz-Martinez, Rafael Marin-Lopez and Fernando Pereniguez Garcia, 1-45. Hershey, Pennsylvania: Information Science Reference. https://arxiv.org/ftp/arxiv/papers/1303/1303.4814.pdf.

Shaftan, Vera. 2015 (Posted on 23 Jul. 2015). "Russia Signs Controversial 'Right to be Forgotten' Bill Into Law." *Data Protection Report.* http://www.dataprotectionreport.com/2015/07/russia-signs-controversial-right-to-be-forgotten-bill-into-law/.

Shim, Elizabeth. 2015 (Posted on 20 Oct. 2015). "Spy agency: North Korea Hackers Stole Sensitive South Korean Data." *UPI: Top News/World News.* http://www.upi.com/Top_News/World-News/2015/10/20/Spy-agency-North-Korea-hackers-stole-sensitive-South-Korean-data/9041445353950/.

Shore, Malcolm, Yi Du and Sherali Zeadally. 2011. "A Public-Private Partnership Model for National Cybersecurity." *Policy & Internet* 3(2). http://onlinelibrary.wiley.com/doi/10.2202/1944-2866.1114/pdf.

Siegfried, Jason, Christine Siedsma, Bobbie-Jo Countryman and Chester D. Hosmer. 2004. "Examining the Encryption Threat." *International Journal of Digital Evidence* 2(3). https://www.utica.edu/academic/institutes/ecii/publications/articles/A0B0C4A4-9660-B26E-12521C098684EF12.pdf.

Silverman, Craig & Lawrence Alexander. 2016 (Posted on 3 Nov. 2016). "How Teens in the Balkans Are Duping Trump Supporters with Fake News." *Buzzfeed News.* https://www.buzzfeed.com/craigsilverman/how-macedonia-became-a-global-hub-for-pro-trump-misinfo?utm_term=.eiWv81lZY#.yrrb4qwgD.

Silverstone, Roger. 2006. *Media and morality on the rise of the Mediapolis.* New York: Wiley.

Simmons, Luke. 2015 (Posted on 14 Oct. 2015). "What Is the Difference between the Internet of Everything and the Internet of Things." *CloudRail.* https://cloudrail.com/internet-of-everything-vs-internet-of-things/.

Simson, Caroline. 2015 (Posted on 27 Mar. 2015). "Australia OKs Data Retention Bill despite Privacy Concerns." *Law360.* https://www.law360.com/articles/636319/australia%20oksdataretentionbilldespiteprivacyconcerns.

Singh, Abhishek Pratap. 2016 (Posted on 23 Dec. 2016). "China's First Cyber Security Law." *Institute for Defense Studies and Analyses.* http://www.idsa.in/backgrounder/china-first-cyber-security-law_apsingh_231216#footnote5_w4sr2kl.

Smale, Alison & Michael D. Shearmarch. 2014 (Posted on 24 Mar. 2014). "Russia Is Ousted from Group of 8 by US and Allies." *New York Times.* http://www.nytimes.com/2014/03/25/world/europe/obama-russia-crimea.html?_r=0.

Smart Cities Council. "Smart Cities Council." *Smart Cities Council.* http://smartcitiescouncil.com/.

Smith, Brad. 2017 (Posted on 14 May 2017). "The Need for Urgent Collective Action to Keep People Safe Online: Lessons from Last Week's Cyberattack." *Official Microsoft Blog*. https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/#oHaqtHbEYodLhwLl.99.

Smith, Jamie. 2016 (Posted on 9 Nov. 2016). "There Is More to Blockchain than Moving Money. It Has the Potential to Transform Our Lives—Here's How." *World Economic Forum.* https://www.weforum.org/agenda/2016/11/there-is-more-to-blockchain-than-moving-money.

Smith, Russell G., Ray Chak-Chung Cheung, Laurie Yiu-Chung Lau, eds. 2015. *Cybercrime Risks and Responses: Eastern and Western Perspectives*. London: Palgrave MacMillan.

Snow, Gordon M. 2011. Statement before the House Financial Services Committee. Subcommittee on Financial Institutions and Consumer Credit. Washington: FBI. https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector.

Socco, Michele. 2013. "Fight against Cybercrime: a European perspective." In: *Cyber Crime: Risks for the Economy and Enterprises (Proceedings of UNICRI round table),* Lucca, Italy, 29 Nov., 29–32. Turin: UNICRI. http://www.unicri.it/special_topics/securing_cyberspace/current_and_past_activities/current_activities/Lucca_Proceedings.pdf.

Sofaer, Abraham D. and Seymour E. Goodman. 2000. *A Proposal for an International Convention on Cyber Crime and Terrorism.* Stanford: CISAC (Center for International Security and Cooperation). http://cisac.fsi.stanford.edu/sites/default/files/sofaergoodman.pdf.

Solove, Daniel J. 2011. *Nothing to Hide: The False Tradeoff between Privacy and Security*. New Haven: Yale University Press.

Solove, Daniel J. and Paul Schwartz. 2014. *Information Privacy Law* (5th Edition). Frederick: Wolters Kluwer Law & Business.

Sotto, Lisa J. and Aaron P. Simpson. "Data Protection and Privacy 2016." In: *Getting the Deal Through:* 169-175. Washington, D.C.: Hunton & Williams LLP. https://www.hunton.com/files/Publication/5c30013e-fa2d-4f6f-8cf0-1df81bf2209d/Presentation/PublicationAttachment/8ddc7e60-dfd4-4b07-a845-221bb6667921/data-protection-privacy-eu-usa.pdf.

Soukieh, Kim. 2011. "Cybercrime –The Shifting Doctrine of Jurisdiction." *Canberra Law Review* 10: 221-238. http://www.austlii.edu.au/au/journals/CanLawRw/2011/9.pdf.

Spidalieri, Francesca. 2015. *State of the States on Cybersecurity.* Newport: Pell Center for International Relations and Public Policy. http://pellcenter.org/wp-content/uploads/2015/11/Pell-Center-State-of-the-States-Report.pdf.

Stalder, Felix. 1998. "The Logic of Networks: Social Landscapes vis-a-vis the Space of Flows." *Ctheory.net*. http://www.ctheory.net/articles.aspx?id=263.

Stalking Resource Center, National Center for Victims of Crime. 2003. "*Stalking Technology Outpaces State Laws.*" *Stalking Resource Center Newsletter* 3, no. 2. https://victimsofcrime.org/docs/src/stalking-technology-outpaces-state-laws17A308005D0C.pdf?sfvrsn=2.

State of New Jersey/Department of Law & Safety, Division of Criminal Justice. 2000. *New Jersey: Computer Evidence Search and Seizure Manual.* Trenton: State of New Jersey/Department of Law & Public Safety, Division of Criminal Justice. www.state.nj.us/lps/dcj/pdfs/cmpmanfi.pdf.

Statista. Number of Internet Users Worldwide from 2000 to 2015 (in Millions)." Statista. http://www.statista.com/statistics/273018/number-of-internet-users-worldwide/.

Steel, Alex. 2010. "The True Identity of Australian Identity Theft Offences: A Measured Response or an Unjustified Status Offence?" *University of New South Wales Law Journal* Vol. 33: 503 –531.

Stephenson, P. 2003. "A Comprehensive Approach to Digital Incident Investigation." *Information Security Technical Report* 8(2): 42-54.

Stone, Kolvin, Christian Schröder, Antony P. Kim & Aravind Swaminathan. 2015 (Posted 6 Oct. 2015). "US–EU Safe Harbor – Struck Down!" *Orrick Trust Anchor Blog*. http://blogs.orrick.com/trustanchor/2015/10/06/us-eu-safe-harbor-struck-down/.

Sturges, Paul. 2006. "Limits to Freedom of Expression? Considerations Arising from the Danish Cartoons Affair" *IFLA Journal* 32 (3): 181-188. http://www.ifla.org/files/assets/faife/publications/sturges/cartoons.pdf.

Sullivan, Bob. 2001 (Posted on 20 Nov. 2001). "FBI Software Cracks Encryption Wall." *NBC News*. http://www.nbcnews.com/id/3341694/ns/technology_and_science-security/t/fbi-software-cracks-encryption-wall/#.V0DuWTotBjo.

Supreme People's Court and Supreme People's Procuratorate. 2004. "Interpretation of Some Questions on Concretely Applicable Law in the Handling of Criminal Cases of Using the Internet or Mobile Communication Terminals and Voicemail Platforms to Produce, Reproduce, Publish, Peddle or Disseminate Obscene Electronic Information." *China Copyright and Media*. https://chinacopyrightandmedia.wordpress.com/2004/09/09/interpretation-of-some-questions-on-concretely-applicable-law-in-handling-criminal-cases-of-using-the-internet-or-mobile-communication-terminals-and-voicemail-platforms-to-produce-reproduce-publish-2/#more-1700.

Sweeney, Brendan J. 2008. "Global Competition: Searching For a Rational Basis for Global Competition Rules." *Sydney Law Review* 30: 209 –244. https://sydney.edu.au/law/slr/slr30_2/Sweeney.pdf.

Swire, Peter and Lauren Steinfeld. 2002. "Security and Privacy after September 11: The Health Care Example." *Minnesota Law Review* 86(6):1515-1540. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=347322.

Symantec Corporation. 2014. *Internet Security Threat Report 2014: Volume 19.* Mountain View: Herndon, Virginia: Symantec Corporation. http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf.

Symantec Corporation. 2015. *Norton Cybersecurity Insights Report.* Herndon, Virginia: Symantec Corporation. https://us.norton.com/norton-cybersecurity-insights-report-global?inid=hho_norton.com_cybersecurityinsights_hero_seeglobalrpt.

Symantec Corporation. 2016. *Norton Cybersecurity Insights Report.* Herndon, Virginia: Symantec Corporation. https://us.norton.com/norton-cybersecurity-insights-report-global?inid=hho_norton.com_cybersecurityinsights_hero_seeglobalrpt.

Symanetc Corporation. 2017. 2017 *Internet Security Threat Report.* Herndon, Virginia: Symantec Corporation. https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf.

Symantec Security Response. 2017 (Posted on 22 May 2017). "WannaCry: Ransomware Attacks Show Strong Links to Lazarus Group." *Symantec Official Blog.* https://www.symantec.com/connect/blogs/wannacry-ransomware-attacks-show-strong-links-lazarus-group.

T

Tabo, Tamara. 2015 (Posted on 12 Jun. 2015). "United States v. The Internet: America's Most Wanted May Look a Lot Like You." *Above the Law.* http://abovethelaw.com/2015/06/united-states-v-the-internet-americas-most-wanted-may-look-a-lot-like-you/.

Tamarkin, Eric. 2015 (Posted on Jan. 2015). "The AU's Cybercrime Response: A Positive Start, but Substantial Challenges Ahead." *Institute for Security Studies.* https://www.files.ethz.ch/isn/187564/PolBrief73_cybercrime.pdf.

Tapscott, Don. & Alex Tapscott. 2016 (Posted on 10 May 2016). "The Impact of the Blockchain Goes Beyond Financial Services." *Harvard Business Review.* https://hbr.org/2016/05/the-impact-of-the-blockchain-goes-beyond-financial-services.

Taylor, Paul. 2001. "The Scope of Government Access to Copies of Electronic Communication Stored with Internet Service Providers: A Review of Legal Standards." *Journal of Technology Law and Policy* 6(2): 109-174.

Talleur, Tom. 2002. "Digital Evidence: The Moral Challenge." *International Journal of Digital Evidence* 1(1). https://www.utica.edu/academic/institutes/ecii/publications/articles/9C4E398D-0CAD-4E8D-CD2D38F31AF079F9.pdf.

Tendulkar, Rohini. 2013. "Cyber-crime, Securities Markets and Systemic Risk." Joint Staff Working Paper of the IOSCO Research Department and World Federation of Exchanges, ICSCO, Madrid. http://www.iosco.org/research/pdf/swp/Cyber-Crime-Securities-Markets-and-Systemic-Risk.pdf.

The Bible, Mat. 9:16–17 (NRSV).

The Commonwealth. "About Us." *The Commonwealth.* http://thecommonwealth.org/about-us.

The Commonwealth. "Commonwealth Cybercrime Initiative." *The Commonwealth.* http://thecommonwealth.org/commonwealth-cybercrime-initiative.

The Commonwealth. 2014. "The Commonwealth Cybercrime Initiative: A Quick Guide." *The Commonwealth.* http://www.securityskeptic.com/CCI%20Quick%20Guide.pdf.

The Commonwealth. 5–8 May 2014. "Communiqué: Commonwealth Law Ministers Meeting." *The Commonwealth.* http://thecommonwealth.org/media/news/communique-commonwealth-law-ministers-meeting-2014#sthash.oZZBUeVU.dpuf.

The Commonwealth. (16–18 Mar. 2016). "Gros Islet Communiqué." The Caribbean Stakeholders Meeting on Cybersecurity and Cybercrime (CSM-II) Commonwealth. http://thecommonwealth.org/sites/default/files/news-items/documents/6%20FinalCastriesDeclaration170316.pdf.

The Commonwealth. 2016 (Posted on15 Mar. 2016). "Caribbean to Tackle Escalating Cybercrime with Regional Approach." *The Commonwealth.* http://thecommonwealth.org/media/press-release/caribbean-tackle-escalating-cybercrime-regional-approach#sthash.HjmhE8I8.dpuf.

The Economist. 2012. (Posted on 11 Feb. 2012). "Indian Telecoms Scandal: Megahurts." *The Economist.* http://www.economist.com/node/21547280.

The Egmont Group. 2015. *The Egmont Group Strategic Plan 2014 – 2017.* Toronto: The Egmont Group. http://www.egmontgroup.org/library/download/415.

The Rt Hon Matt Hancock MP, UK Cabinet Office & UK National Security Secretariat. 2016. "UK Cyber Security Strategy: Statement on the Final Annual Report." *GOV.uk.* https://www.gov.uk/government/speeches/uk-cyber-security-strategy-statement-on-the-final-annual-report.

The White House. 2012. *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy.* Washington, D.C.: The White House. https://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

The White House. 2012. *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure.* Washington, D.C.: The White House. https://www.dhs.gov/sites/default/files/publications/Cyberspace_Policy_Review_final_0.pdf.

The White House of President Barack Obama. "1 is 2 Many: Resources Violence Against Women Act." *The White House of President Barack Obama.* https://obamawhitehouse.archives.gov/1is2many.

The White House of President Barack Obama. "Factsheet: The Violence Against Women Act." *The White House of President Barack Obama.* https://obamawhitehouse.archives.gov/sites/default/files/docs/vawa_factsheet.pdf.

The White House of President Barack Obama. "Electronic Crimes Task Forces (ECTF)." *The White House of President Barack Obama.* https://obamawhitehouse.archives.gov/files/documents/cyber/United%20States%20Secret%20Service%20-%20Electronic%20Crimes%20Task%20Forces.pdf.

The White House of Barack Obama. 2015 (Posted on 13 Feb. 2015). "Executive Order -- Promoting Private Sector Cybersecurity Information Sharing." *The White House of President Barack Obama.* https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari

Threatcloud. "Live Cyber Attack Threat Map." *Threatcloud.* https://threatmap.checkpoint.com/ThreatPortal/livemap.html.

Tiernan, B. 2000. *E-tailing.* Chicago: Dearborn.

Tor Project. "Tor." *Tor Project.* https://torproject.org/.

Tosza, Stanislaw. 2013. "Online Social Networks and Violations Committed Using I.T. –Identity Fraud and Theft of Victual Property." *International Review of Penal Law* 84:115–139.

Tsukayama, Hayley. 2014 (Posted on 13 Nov. 2014). "Facebook Rewrites Its Privacy Policy so that Humans Can Understand It." *The Washington Post.* https://www.washingtonpost.com/news/the-switch/wp/2014/11/13/facebook-rewrites-its-privacy-policy-so-that-humans-can-understand-it/.

Turnbull, Benjamin, Barry Blundell and Jill Slay. 2006. "Google Desktop as a Source of Digital Evidence." *International Journal of Digital Evidence* 5(1). https://www.utica.edu/academic/institutes/ecii/publications/articles/EFE47BD9-A897-6585-5EAB032ADF89EDCF.pdf.

U

U.K. (United Kingdom) Cabinet Office and UK National Security Secretariat. 2011. "The UK Cyber Security Strategy—Protecting and Promoting the UK in a Digital World." London: Crown. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf.

U.K. Cabinet Office and UK National Security Secretariat. 2013. "Cyber Security Strategy: Progress So Far." London: Crown. https://www.gov.uk/government/collections/cyber-security-strategy-progress-so-far--2.

U.K. Cabinet Office & UK National Security Secretariat. 2016. "The UK Cyber Security Strategy 2011-2016: Annual Report." *Gov.uk.* https://www.gov.uk/government/publications/the-uk-cyber-security-strategy-2011-2016-annual-report.

U.K. Home Office. 2016. *Investigatory Powers Bill: Explanatory Notes to the Investigatory Powers Bill as brought from the House of Commons on 8 June 2016 (HL Bill 40).* https://www.publications.parliament.uk/pa/bills/lbill/2016-2017/0040/17040en.pdf.

U.K. Home Secretary. 2017 (Posted on 26 Mar. 2017). 'We need the Help of Social Media Companies." *UK Home Office News Team.* https://homeofficemedia.blog.gov.uk/2017/03/26/home-secretary-we-need-the-help-of-social-media-companies/.

U.K. NCA (National Crime Agency). 2014 (Posted on 19 May. 2014). "Unprecedented UK Operation Aids Global Strike against Blackshades Malware." *NCA.* http://www.nationalcrimeagency.gov.uk/news/news-listings/371-uk-arrests-in-international-operation.

U.K. Parliament. "Investigatory Powers Act 2016." *U.K. Parliament.* http://services.parliament.uk/bills/2015-16/investigatorypowers.html.

UN (United Nations). 2000. "Crime Related to Computer Networks: Background Paper for the Workshop on Crimes Related to Computer Networks." A/CONF.187/10. Paper prepared for the 10th UN Congress on the Prevention of Crime and Treatment of Offenders, "Crime and Justice: Meeting the Challenges of the Twenty-first Century," Vienna, 10-17 April. http://www.un.org/ga/search/view_doc.asp?symbol=A/CONF.187/10.

UN. 2006. "Annex E. Extraterritorial Jurisdiction." In: *Report of the International Law Commission: Fifty-eighth session (1 May-9 June and 3 July-11 August 2006),* 516-40. A/61/10. New York: UN. http://legal.un.org/ilc/documentation/english/reports/a_61_10.pdf.

UN. 2010. "Working Paper Prepared by the Secretariat on Recent Developments in the Use of Science and Technology by Offenders and by Competent Authorities in Fighting Crime, including the Case of Cybercrime." A/CONF.213/9. Paper prepared for the 12th UN Congress on Crime Prevention and Criminal Justice, "Comprehensive strategies for global challenges: crime prevention and criminal justice systems and their development in a changing world," Salvador, 12-19 April. http://www.un.org/ga/search/view_doc.asp?symbol=A/CONF.213/9.

UN. 2014. "The Obligation to Extradite or Prosecute." *Final Report of the UN International Law Commission.* http://legal.un.org/ilc/texts/instruments/english/reports/7_6_2014.pdf

UN. 2015. "Background Paper on the Workshop on Strengthening Crime Prevention and Criminal Justice Responses to Evolving Forms of Crime, such as Cybercrime and Trafficking in Cultural Property, including Lessons Learned and International Cooperation." A/CONF.222/12. Paper prepared for the 13th UN Congress on Crime Prevention and Criminal Justice, "Integrating crime prevention and criminal justice into the wider UN agenda to address social and economic challenges and to promote the rule of law at the national and international levels and public participation," Doha, 12-19 April. http://www.un.org/ga/search/view_doc.asp?symbol=A/CONF.222/12.

UN. 2015. "Draft Doha Declaration on Integrating Crime Prevention and Criminal Justice into the Wider United Nations Agenda to Address Social and Economic Challenges and to Promote the Rule of Law at the National and International Levels and Public Participation." A/CONF.222/L.6. Paper prepared for the 13th UN Congress on Crime Prevention and Criminal Justice, "Integrating crime prevention and criminal justice into the wider UN agenda to address social and economic challenges and to promote the rule of law at the national and international levels and public participation," Doha, 12-19 April. http://www.un.org/ga/search/view_doc.asp?symbol=A/CONF.222/L.6.

UN. 2015 (Posted on 16 April. 2015). "Public-private Partnerships Needed to Combat Transnational Cyber-crime." *UN/Multimedia*. http://www.unmultimedia.org/radio/english/2015/04/public-private-partnerships-needed-to-combat-transnational-cyber-crime/#.V0XQ0IcUU5u.

UN. "Secretriat." *UN*. http://www.un.org/en/sections/about-un/secretariat/index.html.

UN Commission on Human Rights. 1999. *Report of the Special Rapporteur on the Protection and Promotion of the Right to Freedom of Opinion and Expression, Mr. Abid Hussain.* E/CN.4/1999/64. New York: UN. http://dag.un.org/bitstream/handle/11176/223391/E_CN.4_1999_64-EN.pdf?sequence=3&isAllowed=y.

UN Commission on Human Rights. 1995. *Promotion and protection of the right to freedom of opinion and expression Report of the Special Rapporteur, Mr. Abid Hussain, pursuant to Commission on Human Rights resolution 1993/45* (E/CN.4/1995/32). New York: UN. https://documents-dds-ny.un.org/doc/UNDOC/GEN/G94/750/76/PDF/G9475076.pdf?OpenElement.

UN Committee against Torture. 2016. "Consideration of reports submitted by States parties under article 19 of the Convention pursuant to the optional reporting procedure." Third to Fifth Periodic Reports of States Parties due in 2012. Korea: UN. http://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2FPPRiCAqhKb7yhsvF6hiQLJAnpG6iplFwLNHHRo0OD78WS4LFAhS78ybK9cAdJ5ZfbR4liAXIyMG4l6gfS%2BNuCz6URY2YsRMgaSD1rC4Di8J1OSunD47yXd4UH.

UN CRC (United Nations Committee on the Rights of the Child). 2010. *Consideration of Reports Submitted by States Parties under Article 12, Paragraph 1, of the Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography, Initial Reports of States Parties Due in 2005, Argentina.* CRC/C/OPSC/ARG/1. Geneva: UN OHCHR. http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=CRC%2FC%2FOPSC%2FARG%2F1&Lang=en.

UNCTAD (UN Conference on Trade and Development). "Data Protection and Privacy Legislation Worldwide." United Nations. http://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx.

UNCTAD. *Information Economy Report 2005.* Geneva: UNCTAD. http://unctad.org/en/docs/sdteedc20051_en.pdf.

UNCTAD. 2012. *Harmonizing Cyberlaws and Regulations: The Experience of the East African Community.* Geneva: UNCTAD. http://unctad.org/en/PublicationsLibrary/dtlstict2012d4_en.pdf.

UNCTAD. 2015. *Information Economy Report 2015: Unlocking the Potential of E-commerce for Developing Countries.* Geneva: UNCTAD. http://unctad.org/en/PublicationsLibrary/ier2015_en.pdf.

UNCTAD. 2016. "Cybercrime Legislation Worldwide." *UNCTAD.* http://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Cybercrime-Laws.aspx.

UNCTAD. "Cyberla Tracker." *UNCTAD.* http://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx.

UNCTAD. "Summary of Adoption of E-Commerce Legislation Worldwide." *UNCTAD.* unctad.org/cyberlawtracker.

UNCTAD. "TrainForTrade." *UNCTAD.* https://tft.unctad.org/?page_id=119.

UNCTAD & Eastern African Community. 2008. "Draft EAC Legal Framework." *The East African Community IRC Repository.* http://repository.eac.int:8080/bitstream/handle/11671/1815/EAC%20Framework%20for%20Cyberlaws.pdf?sequence=1&isAllowed=y.

UN Department of Economic and Social Affairs. 2014. *Open Working Group Proposal for Sustainable Development Goal.* New York: UN. https://sustainabledevelopment.un.org/content/documents/1579SDGs%20Proposal.pdf.

UN Development Programme (UNDP). 2001. *Human Development Report 2001: Making New Technologies Work for Human Development.* New York: United Nations. http://hdr.undp.org/en/content/human-development-report-2001.

UNESCO (United Nations Educational, Scientific and Cultural Organization). 2008. *Medium-Term Strategy for 2008-2013.* Geneva: UNESCO. http://unesdoc.unesco.org/images/0014/001499/149999e.pdf.

UNESCO. 2014. *World Trends in Freedom of Expression and Media Development: Regional Overview of Asia and the Pacific.* Paris: UNESCO. http://unesdoc.unesco.org/images/0022/002277/227737e.pdf.

UNESCO. 2014. *World Trends in Freedom of Expression and Media Development: Regional Overview of Latin America and the Caribbean.* Paris: UNESCO. http://unesdoc.unesco.org/images/0022/002277/227740e.pdf.

UNESCO. 2015. *Keystones to Foster Inclusive Knowledge Societies: Access to information and Knowledge, Freedom of Expression, Privacy and Ethics on a Global Internet.* Paris: UNESCO. http://unesdoc.unesco.org/images/0023/002325/232563E.pdf.

UNESCO. 2016. *Concept Note: Access to Information and Fundamental Freedoms This Is Your Right! (World Press Freedom Day 3 May 2016).* Paris. UNESCO. http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/WPFD/WPFD2016_Concept-Note.pdf.

UN General Assembly. 2011. *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression.* A/66/290.New York: UN. http://www.un.org/ga/search/view_doc.asp?symbol=A/66/290.

UN General Assembly. 2012. *Report of the Special Rapporteur on the Situation of Human Rights Defenders.* A/67/292. New York: UN. http://www.un.org/ga/search/view_doc.asp?symbol=A/67/292.

UN General Assembly. 2015. Report of the Special Rapporteur on the Situation of Human Rights Defenders. A/70/217. New York: UN. http://www.un.org/ga/search/view_doc.asp?symbol=A/70/217.

UN Human Rights Committee. 1988. *Report of the Human Rights Committee –General Assembly Official Records: Forty-third Session Supplement No. 40.* A/43/40.New York: UN. http://www.un.org/en/ga/search/view_doc.asp?symbol=A/43/40.

UN Human Rights Committee. 1999. *General Comments adopted by the Human Rights Committee under Article 40, Paragraph 4, of the International Covenant on Civil and Political Rights.* CCPR/C/21/Rev.1/Add.9. New York: UN. https://documents-dds-ny.un.org/doc/UNDOC/GEN/G99/459/25/PDF/G9945925.pdf?OpenElement.

UN Human Rights Committee. 2014. *Concluding observations on the fourth periodic report of the United States of America.* CCPR/C/USA/CO/4. Geneva: UN OHCHR. http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=CCPR%2fC%2fUSA%2fCO%2f4&Lang=en.

UN Human Rights Committee. 2015. *Concluding observations on the seventh periodic report of the United Kingdom of Great Britain and Northern Ireland.* CCPR/C/GBR/CO/7. Geneva: UN OHCHR. http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=CCPR/C/GBR/CO/7&Lang=En.

UN Human Rights Committee. 2015. *Concluding Observations on the Fifth Periodic Report of France.* CCPR/C/FRA/CO/5. Geneva: UN OHCHR. http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=CCPR/C/FRA/CO/5&Lang=En.

UN Human Rights Council. 2010. *Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, Martin Scheinin: Compilation of Good Practices on Legal and Institutional Frameworks and Measures that Ensure Respect for Human Rights by Intelligence Agencies while Countering Terrorism, Including on Their Oversight.* A/HRC/14/46. New York: UN. https://documents-dds-ny.un.org/doc/UNDOC/GEN/G10/134/10/PDF/G1013410.pdf?OpenElement.

UN Human Rights Council. 2011. *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue.* A/HRC/17/27. New York: UN. https://documents-dds-ny.un.org/doc/UNDOC/GEN/G11/132/01/PDF/G1113201.pdf?OpenElement.

UN Human Rights Council. 2013. *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue.* A/HRC/23/40. New York: UN. https://documents-dds-ny.un.org/doc/UNDOC/GEN/G13/133/03/PDF/G1313303.pdf?OpenElement.

UN Human Rights Council. 2014. *The Right to Privacy in the Digital Age: Report of the Office of the United Nations High Commissioner for Human Rights.* A/HRC/27/37. New York: UN. https://documents-dds-ny.un.org/doc/UNDOC/GEN/G14/088/54/PDF/G1408854.pdf?OpenElement.

UN Human Rights Council. 2015. *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye.* A/HRC/29/32. New York: UN. https://documents-dds-ny.un.org/doc/UNDOC/GEN/G15/095/85/PDF/G1509585.pdf?OpenElement.

UN Human Rights Council. 2016. The Promotion, Protection and Enjoyment of Human Rights on the Internet. A/HRC/32/L.20. http://daccess-ods.un.org/access.nsf/Get?Open&DS=A/HRC/32/L.20&Lang=E.

UNICRI (United Nations Interregional Crime and Justice Research Institute). 2013. "Background Information: How is cybercrime defined?" In: *Cyber Crime: Risks for the Economy and Enterprises [Proceedings of UNICRI round table (Lucca, Italy, 29 November 2013)]*, 7. Turin: UNICRI. http://www.unicri.it/special_topics/securing_cyberspace/current_and_past_activities/current_activities/Lucca_Proceedings.pdf.

UNICRI. 2014. *Cybercrime: Risks for the Economy and Enterprises at the EU and Italian Level*. Turin: UNICRI. http://www.unicri.it/in_focus/files/Criminalita_informatica_inglese.pdf.

UNICRI. 2014. "Information Sharing and Public-Private Partnerships: Perspectives and Proposals." Working Paper. UNICRI, Turin. http://www.unicri.it/special_topics/securing_cyberspace/current_and_past_activities/current_activities/Information_Sharing_cover_INDEXED_0611.pdf.

UNICRI. 2015. *Guidelines for IT Security in SMEs*. Turin: UNICRI. http://www.unicri.it/news/files/Research-Guidelines_for_IT_Security_of_SMEs-Flavia_Zappa_FINAL.pdf.

UNODC (United Nations Office on Drugs and Crime). 2012. *Cybercrime Questionnaire for Member States*. Vienna: UNODC. https://cms.unov.org/DocumentRepositoryIndexer/GetDocInOriginalFormat.drsx?DocID=f4b2f468-ce8b-41e9-935f-96b1f14f7bbc.

UNODC. 2013. *Comprehensive Study on Cybercrime (Draft)*. Vienna: UNODC. http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.

UNODC. 2015. *Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children*. Vienna: UNODC. https://www.unodc.org/documents/organized-crime/cybercrime/Study_on_the_Effects.pdf.

UNODC. 2016 (Posted on 13 Oct. 2016). "UNODC Provided Training to South East Asian Institutions to Combat Cybercrime." *UNODC*. https://www.unodc.org/unodc/en/frontpage/2016/October/unodc-provided-training-to-south-east-asian-institutions-to-combat-cybercrime.html

UNODC. "UNODC Repository on Cyber Crime." *UNODC*. https://www.unodc.org/cld/v3/cybrepo/legdb/index.html?lng=en.

UNODC. "SHERLOC Portal." *UNODC*. https://www.unodc.org/cld/v3/sherloc/.

UN Secretariat. 2015. "Comprehensive and balanced approaches to prevent and adequately respond to new and emerging forms of transnational crime Working paper." A/CONF.222/8. 13th UN Congress on Crime Prevention and Criminal Justice. http://www.unodc.org/documents/congress//Documentation/A-CONF.222-8/ACONF222_8_e_V1500538.pdf.

UN Sustainable Development. "Open Working Group Proposal for Sustainable Development Goals." *UN Sustainable Development*. https://sustainabledevelopment.un.org/focussdgs.html

U.S. (United States) Attorney's Office, N.D. Ga. 2014 (Posted on 28 Jan. 2014). "Cyber Criminal Pleads Guilty to Developing and Distributing Notorious SpyEye Malware." *FBI*. https://archives.fbi.gov/archives/atlanta/press-releases/2014/cyber-criminal-pleads-guilty-to-developing-and-distributing-notorious-spyeye-malware.

U.S. CERT (Computer Emergency Readiness Team. "US-CERT: About Us." *US CERT*. https://www.us-cert.gov/about-us.

U.S. Department of Commerce, Internet Policy Task Force. 2013. *Copyright, Creativity and Innovation in the Digital Economy.* Washington, D.C.: U.S. Department of Commerce. http://www.uspto.gov/sites/default/files/news/publications/copyrightgreenpaper.pdf.

U.S. Department of Defense. "DoD Cyber Crime Center (DC3)." *U.S. Department of Defense.* http://www.dc3.mil/.

U.S. Department of Homeland Security. "Combatting Cyber Crime." *U.S. Department of Homeland Security.* https://www.dhs.gov/topic/combating-cyber-crime.

U.S. Department of Justice. 1989. *Computer Crime: Criminal Justice Resource Manual* (2d ed.). National Institute of Justice, Office of Justice Program. OJP-86-C-002.

U.S. Department of Justice. 1994. "Federal Guidelines for Searching and Seizing Computers." *Bureau of National Affairs, Criminal Law Reporter* Vol. 56. https://epic.org/security/computer_search_guidelines.txt

U.S. Department of Justice. 1996. "Domestic Violence, Stalking, and Antistalking Legislation: An Annual Report to Congress under the Violence Against Women Act." *U.S. Department of Justice, National Institute of Justice.* https://www.fas.org/sgp/crs/misc/R42499.pdf.

U.S. Department of Justice. 2004. *Problem-Oriented Guides for Police Problem-Specific Guides Series Guide: Stalking*, no. 22. *U.S. Department of Justice, National Center for Victims of Crime.* https://victimsofcrime.org/docs/src/stalking-problem-oriented-policiing-guide.pdf?sfvrsn=0.

U.S. Department of Justice. 2004 (Posted on 11 May 2004). "G8 Background." *U.S. Department of Justice.* https://www.justice.gov/ag/g8-background.

U.S. Department of Justice. 2009. *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations.* Washington: Office of Legal Education. https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf.

U.S. Department of Justice. 2010. *Leader of Hacking Ring Sentenced for Massive Identity Theft from Payment Processor and U.S. Retail Networks.* Washington D.C.: U.S. Department of Justice. https://www.justice.gov/sites/default/files/usao-nj/legacy/2014/09/02/dojgonzalez0326rel.pdf.

U.S. Department of Justice. 2016 (Posted on 7 Dec. 2016). "Assistant Attorney General Leslie R. Caldwell Delivers Remarks Highlighting Cybercrime Enforcement at Center for Strategic and International Studies." Office of Public Affairs, U.S. Department of Justice. https://www.justice.gov/opa/speech/assistant-attorney-general-leslie-r-caldwell-delivers-remarks-highlighting-cybercrime.

U.S. Department of Justice. 2016 (Posted on 26 Apr. 2016). "Two Major International Hackers Who Developed the 'SpyEye' Malware Get Over 24 Years Combined in Federal Prison." US Dept. of Justice. https://www.justice.gov/usao-ndga/pr/two-major-international-hackers-who-developed-spyeye-malware-get-over-24-years-combined.

U.S. Department of Justice. 2016 (Posted on 6 Jun. 2016). "Assistant Attorney General Leslie R. Caldwell Speaks at the CCIPS-CSIS Cybercrime Symposium 2016: Cooperation and Electronic Evidence Gathering Across Borders." *U.S. Department of Justice.* https://www.justice.gov/opa/speech/assistant-attorney-general-leslie-r-caldwell-speaks-ccips-csis-cybercrime-symposium-2016.

U.S. Department of Justice, Office of Public Affairs. 2017 (Posted on 15 Mar. 2017). "U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts." *U.S. Department of Justice*. https://www.justice.gov/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions

U.S. Department of Justice. "Agencies." *U.S. Department of Justice*. https://www.justice.gov/agencies/list.

U.S. Department of Justice. "Computer Crime & Intellectual Property Section (CCIPS): About the Computer Crime & Intellectual Property Section." *U.S. Department of Justice*. https://www.justice.gov/criminal-ccips.

U.S. Department of State. 2013 (Posted on 11 Apr. 2013), "Media Note: G8 Foreign Ministers' Meeting Statement," *Office of the Spokesperson, U.S. Department of State*. http://www.state.gov/r/pa/prs/ps/2013/04/207354.htm.

U.S. Department of State, Bureau of Counterterrorism. 2014. "Ch. 5: Terrorist Safe Havens." in: *Country Reports on Terrorism*. http://www.state.gov/j/ct/rls/crt/2014/239412.htm.

U.S. FTC (Federal Trade Commission). 2013. "Mobile Privacy Disclosures: Building Trust through Transparency." Washington, D.C.: U.S. FTC. https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf.

U.S. FTC. 2015. "Internet of Things: Privacy and Security in a Connected World." *FTC Staff Report.* https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

U.S. FTC. 2015. *Statement of Enforcement Principles Regarding "Unfair Methods of Competition" Under Section 5 of the FTC Act.* Washington, D.C.: U.S. FTC. https://www.ftc.gov/system/files/documents/public_statements/735201/150813section5enforcement.pdf.

U.S. GAO (Government Accountability Office). 2007. *Public and Private Entities Face Challenges in Addressing Cyber Threats.* Washington, D.C.: U.S. GAO. http://www.gao.gov/new.items/d07705.pdf.

U.S. Legal.com. "Double Criminality Law & Legal Definition." U*.S. Legal.com*. http://definitions.uslegal.com/d/double-criminality/.

U.S. State of Maryland. *General Guidelines for Seizing Computers and Digital Evidence*. US State of Maryland, Maryland State Police. https://www.coursehero.com/file/8005384/Article-Maryland-Seize-Computers-1/.

University of Oxford–Oxford Martin School, GCSCC (Global Cyber Security Capacity Centre). 2014. *Cyber Security Capability Maturity Model (CMM) – Pilot*. London: University of Oxford–Oxford Martin School, GCSCC. http://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM%20Pilot%20version%20A.15.12.2014.pdf.

Urbas, Gregor. 2012. "Cybercrime, Jurisdiction and Extradition: The Extended Reach of Cross-Border Law Enforcement." *Journal of Internet Law* 16 (1): 7-17.

V

Vaidyanathan, A. 2015. "Supreme Court Reserves Orders on Validity of Section 66A of IT Act." NDTV, 28 Feb. http://www.ndtv.com/india-news/supreme-court-reserves-orders-on-validity-of-section-66a-of-it-act-742758.

Vacca, John R. 2005. *Computer Forensics, Computer Crime Scene Investigation* (2nd Edition). Newton Centre: Charles River Media.

Vaciago, Giuseppe. 2012. *Digital Evidence*. Torino: Giappichelli.

Venmo. "Fees & Venmo." Venmo. https://help.venmo.com/hc/en-us/articles/224361007-Fees-Venmo.

Verini, James. 2010. (Posted on 10 Nov. 2010). "The Great Cyberheist." *New York Times Magazine*. http://www.nytimes.com/2010/11/14/magazine/14Hacker-t.html.

Verizon. 2017. *2017 Data Breach Investigations Report*, 10th ed. Verizon. http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/.

Viano, Emilio C. 2006. "Cybercrime: A New Frontier in Criminology." *International Annals of Criminology* 44 (1/2): 11-22.

Viano, Emilio C. 2012. "Balancing Liberty and Security Fighting Cybercrime: Challenges for the Networked Society." In: *Cybercriminality: Finding a Balance between Freedom and Security,* edited by Stefano Manacorda. 33-63. Milano: ISPAC (International Scientific and Professional Advisory Council) of the United Nations Crime Prevention and Criminal Justice Programme. http://ispac.cnpds.org/download.php?fld=pub_files&f=ispacottobre2012bassa.pdf.

Viano, Emilio C. 2013. "Section 2: Concept Paper and Questionnaire." Paper Prepared for IAPL's Preparatory Colloquium Section II for the 20th International Congress of Penal Law on Information Society and Penal Law, "Criminal Law Special Part," Moscow, 24-27 Apr. http://www.penal.org/IMG/pdf/Section_II_EN.pdf.

Viano, Emilio C. 2013. "Section II – Criminal Law. Special Part. Information Society and Penal Law: General Report." *International Review of Penal Law* 84: 335 – 355.

Villasenor, John. 2016 (Posted on 25 Aug. 2016). "Ensuring Cybersecurity in Fintech: Key Trends and Solutions." *Forbes*. http://www.forbes.com/sites/johnvillasenor/2016/08/25/ensuring-cybersecurity-in-fintech-key-trends-and-solutions/#13edc74be1fa.

Vodaphone. 2016 (Posted on 25 Apr. 2016). "Vodafone M-Pesa Reaches 25 Million Customers Milestone." *Vodaphone*. https://www.vodafone.com/content/index/media/vodafone-group-releases/2016/mpesa-25million.html.

von Spakovsky, Hans A. "The Dangers of Internet Voting." *The Heritage Foundation.* http://www.heritage.org/research/reports/2015/07/the-dangers-of-internet-voting.

Voreacos, David. 2015 (Posted on 13 Feb. 2015). "Accused Moscow Hacker Drinkman arrives in the U.S. for trial." *Bloomberg Business*. http://www.bloomberg.com/news/articles/2015-02-13/accused-moscow-hacker-drinkman-arrives-in-u-s-to-face-trial.

W

Wakefield, Jane. 2005 (Posted on 28 Jul. 2005). "Wireless Hijacking Under Scrutiny." *BBC*. http://news.bbc.co.uk/2/hi/technology/4721723.stm.

Walden, Ian. 2007. *Computer Crimes and Digital Investigations.* London: Oxford University Press. http://www.stephenmason.eu/pdf/book-review-2008.pdf.

Walden, Ian. 2016. *Computer Crimes and Digital Investigations* (2d ed.). Oxford: Oxford University Press.

Walden, Ian. 24–28 Apr. 2017. "Cybersecurity and Cybercrime: New Tools for Better Cyber Protection." UNTAD e-Commerce Week. Geneva: UNCTAD. http://unctad.org/meetings/en/Presentation/dtl_eWeek2017p07_IanWalden_en.pdf.

Walker, Frank. 2008 (23 Mar. 2008). "How Police Broke Net Pedophile Ring." *Sydney Morning Herald*. http://www.smh.com.au/news/national/how-police-broke-net-pedophile-ring/2008/03/22/1205602728709.html.

Walker, Peter & Heather Stewart. 2017 (Posted on 27 Mar. 2017). "No 10 Repeats Rudd's Call for Authorities to Access Encrypted Messages." *Guardian*. https://www.theguardian.com/politics/2017/mar/27/downing-street-amber-rudd-authorities-access-encrypted-messages-whatsapp-terrorism.

Wall, David. 1999. "Cybercrimes: New Wine, No Bottles?" In: Pamela Davies, Peter Francis & Victor Jupp (eds.), *Invisible Crimes: Their Victims and their Regulation*. New York: Macmillan.

Wall, David S. 2001. "Cybercrimes and the Internet." In: *Crime and the Internet* edited by David S. Wall, 1 –17. New York: Routledge.

Wall, David S. 2007. Cybercrime: *The Transformation of Crime in the Information Age*. Cambridge: Polity Press.

Wall, David S. 2007 (published in 2007, as well as revised in 2010 and 2011). "Policing Cybercrimes: Situating the Public Police in Networks of Security within Cyberspace." *Police Practice & Research: An International Journal:* 183 to 205. http://www.cyberdialogue.ca/wp-content/uploads/2011/03/David-Wall-Policing-CyberCrimes.pdf.

Wall, David S. 2008. "Cybercrime, Media and Insecurity: The Shaping of Public Perceptions of Cybercrime." *International Review of Law, Computers and Technology –Crime and Criminal Justice* 22 (1-2): 45-63.

Wall, David S. 2015. "Cybercrime as a Conduit for Criminal Activity." In: *Information Technology and the Criminal Justice System* edited by April Pattavina, 77-98. Beverly Hills, California: Sage Publications.

Weber, Amalie M. 2003. "The Council of Europe's Convention on Cybercrime." *Berkeley Technology Law Journal* 18(1): 425-446.http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1416&context=btlj.

Weber, Max. 1946. "Politics as a Vocation." Max Weber: Essays in Sociology. Oxford: Oxford University Press. http://polisci2.ucsd.edu/foundation/documents/03Weber1918.pdf.

Webster, Stephen, et al. 2012. *European Online Grooming Project: Final Report*. European Online Grooming Project. http://www.europeanonlinegroomingproject.com/media/2076/european-online-grooming-project-final-report.pdf.

Weigend, Thomas. 2012. "Section 1: Concept Paper and Questionnaire." Paper prepared for IAPL's Preparatory Colloquium Section I for the 20th International Congress of Penal Law on Information Society and Penal Law, "Criminal Law General Part," Verona, 28-30 November. http://www.penal.org/IMG/pdf/Section_I_EN.pdf.

Weigend, Thomas. 2013. "Section I – Criminal Law General Part. Information Society and Penal Law: General Report." *International Review of Penal Law* (Vol. 84): 51-75. http://www.penal.org/spip/IMG/SECTION%20I%20General%20Report%20EN.pdf.

Weil, Michael C. 2002. "Dynamic Time & Date Stamp Analysis." *International Journal of Digital Evidence* 1(2). https://www.utica.edu/academic/institutes/ecii/publications/articles/A048B1E4-B921-1DA3-EB227EE7F61F2053.pdf.

Weisser, Bettina. "Cyber Crime—The Information Society and Related Crimes." *Penal*. http://www.penal.org/sites/default/files/files/RM-8.pdf.

Weisser, Carolin. 2015 (Posted on 4 Nov. 2015). "Eastern African Criminal Justice Network on Cybercrime and Electronic Evidence." Cybersecurity Capacity Portal, Oxford University. https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/eastern-african-criminal-justice-network-cybercrime-and-electronic-evidence.

Wendt, Rudolf. 2013. "The Principle of 'Ultima Ratio' and/or the Principle of Proportionality." *Oñate Socio-Legal Series* 3(1): 81 –94. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2200873.

Westbrook, Theodore J. 2006. "Owned: Finding a Place for Virtual World Property Rights." *Michigan State Law Review:* 779-812

Westby, Jody R. 2003. *ABA International Guide to Combating Cybercrime*. Chicago: ABA.

Whitcomb, Carrie Morgan. 2002. "An Historical Perspective of Digital Evidence: A Forensic Scientist's View." *International Journal of Digital Evidence* 1(1). https://www.utica.edu/academic/institutes/ecii/publications/articles/9C4E695B-0B78-1059-3432402909E27BB4.pdf.

Wigmore, John H. 1904. "The History of the Hearsay Rule." *Harvard Law Review* 17, no. 7.

Williams, Pete. 2016 (Posted on 25 May 2016). "Guccifer, Hacker Who Says He Breached Clinton Server, Pleads Guilty." *NBC News*. http://www.nbcnews.com/news/us-news/guccifer-hacker-who-says-he-breached-clinton-server-pleads-guilty-n580186.

Wilson, Clay 2007 (Published in 2007 and Updated in 2008). *Botnets, Cybercrime and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress*. Washington D.C.:U.S. Department of State. http://www.fas.org/sgp/crs/terror/RL32114.pdf.

Winfree, Jr., Thomas, G. Larry Mays & Leanne Fiftal Alarid. 2015. *Introduction to Criminal Justice*. New York: Wolters Kluwer.

Woo, Christopher and Miranda So. 2002. "The Case for Magic Lantern: September 11 Highlights the Need for Increased Surveillance." *Harvard Journal of Law & Technology* 15(2): 521 –538. http://jolt.law.harvard.edu/articles/pdf/v15/15HarvJLTech521.pdf.

Woollacott, Emma. 2016 (Posted on 16 Nov. 2016). "UK Joins Russia and China in Legalizing Bulk Surveillance." *Forbes*. https://www.forbes.com/sites/emmawoollacott/2016/11/16/uk-joins-russia-and-china-in-legalizing-bulk-surveillance/#718b3a2b58ca.

Woollaston, Victoria. 2017 (Posted on 16 May 2017). "Wanna Decryptor Ransomware Appears to be Spawning and This Time It May Not Have a Kill Switch." *Wired*. http://www.wired.co.uk/article/wanna-decryptor-ransomware.

Working to Halt Online Abuse. "U.S. Laws." *Working to Halt Online Abuse*. http://www.haltabuse.org/resources/laws/.

World Bank. 2014. "Comoros Policy Notes: Accelerating Economic Development in the Union of Comoros." Washington D.C.: World Bank.

World Bank. 2015 (Posted on 8 Jan. 2015). "Brief: Smart Cities." World Bank. http://www.worldbank.org/en/topic/ict/brief/smart-cities.

World Bank. 2016. *World Development Report 2016: Digital Dividends*. Washington, DC: World Bank. https://openknowledge.worldbank.org/handle/10986/23347.

WEF (World Economic Forum). 2016. *Recommendations for Public-Private Partnership against Cybercrime*. Geneva: WEF. http://www3.weforum.org/docs/WEF_Cybercrime_Principles.pdf.

Y

Yadron, Danny, Spencer Ackerman and Sam Thielman. 2016 (Posted on 18 Feb. 2016). "Inside the FBI's Encryption Battle with Apple." *The Guardian*. https://www.theguardian.com/technology/2016/feb/17/inside-the-fbis-encryption-battle-with-apple.

Yan, Sophia. & K.J. Kwon. 2014 (Posted on 21 Jan. 2014). "Massive Data Theft Hits 40% of South Koreans." *CNN Tech*. http://money.cnn.com/2014/01/21/technology/korea-data-hack/.

Yar, Majid. 2005. "The novelty of 'cybercrime': An assessment in light of routine activity theory." *European Society of Criminology* 2 (4): 407-27.

Yonhap. 2015 (Posted on 12 Mar. 2015)."Hacker Demands Money for Information on S. Korean Nuclear Reactors." *Yonhap*. http://english.yonhapnews.co.kr/national/2015/03/12/40/0302000000AEN20150312008051320F.html

Z

Zappa, Flavia. 2014. *Cyber Crime: Risks for the Economy and Enterprises at the EU and Italian Level*. Turin: UNICRI. http://www.unicri.it/in_focus/files/Criminalita_informatica_inglese.pdf.

Završnik, Aleš. 2010. "Towards an Overregulated Cyberspace." *Masaryk University Journal of Law & Technology* 4(2): 173-190. https://journals.muni.cz/mujlt/article/viewFile/2566/2130.

Zetter, Kim. 2011 (Posted on 7 Apr. 2011). "In Surprise Appeal, TJX Hacker Claims U.S. Authorized His Crimes." *Wired*. http://www.wired.com/2011/04/gonzalez-plea-withdrawal/.

Zetter, Kim. 2014. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. New York: Crown Publishers.

Zetter, Kim. 2014 (Posted on 28 Jan. 2014). "Coder Behind Notorious Bank-hacking Tool Pleads Guilty." *Wired*. http://www.wired.com/2014/01/spy-eye-author-guilty-plea/.

Zetter, Kim. 2014 (Posted on 15 Apr. 2014). "Obama: NSA Must Reveal Bugs Like Heartbleed, Unless They Help the NSA," *Wired*. https://www.wired.com/2014/04/obama-zero-day/.

Zetter, Kim. 2014 (Posted on 3 Nov. 2014). "An Unprecedented Look at Stuxnet, the World's First Digital Weapon." *Wired*. https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

Zetter, Kim. 2016 (Posted on 8 Apr. 2016). "The Feds' Battle with Apple Isn't Over—It Just Moved to New York." *Wired*. https://www.wired.com/2016/04/feds-battle-apple-isnt-just-moved-ny/.

Zorabedian, John. 2016 (Posted on 18 Jan. 2016). "Ross Ulbricht Appeals Silk Road Conviction—-Did He Get a Fair Trial?" *Naked Security*. https://nakedsecurity.sophos.com/2016/01/18/ross-ulbricht-appeals-silk-road-conviction-did-he-get-a-fair-trial/.

Zuckerberg, Mark. 2013. "Is Connectivity a Human Right?" *Facebook*. https://www.facebook.com/isconnectivityahumanright.

Multilateral Instruments

Treaties, Directives, Additional Protocols and Resolutions, etc

African Union. 2014 (Adopted on 27 Jun. 2014). African Union Convention on Cyber Security and Personal Data Protection. https://www.au.int/web/en/treaties/african-union-convention-cyber-security-and-personal-data-protection.

ASEAN (Association of Southeast Asian Nations). 2012. ASEAN Human Rights Declaration.

CIS (Commonwealth of Independent States). 2001 (Done on 1 Jun. 2001). Agreement on cooperation among the States members of the Commonwealth of Independent States in Combating Offences related to Computer Information. https://cms.unov.org/documentrepositoryindexer/GetDocInOriginalFormat.drsx?DocID=5b7de69a-730e-43ce-9623-9a103f5cabc0.

Council of Europe. 1950 (Opened for Signature on 4 Nov. 1950). Convention for the Protection of Human Rights and Fundamental Freedoms (also known as "European Convention on Human Rights"). https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680063765.

Council of Europe. 1957. European Convention on Extradition. Paris, ETS No. 24. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/024.

Council of Europe. 1981 (Opened for Signature on 28 Jan. 1981). Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680078b37.

Council of Europe. 2001 (Opened for Signature on 23 Nov. 2001). Convention on Cybercrime. http://conventions.coe.int/treaty/en/treaties/word/185.doc.

Council of Europe. 2003 (Opened for signature on 28 Jan. 2003). Additional Protocol to Convention on Cybercrime Concerning the Criminalization of Acts of a Racist and Xenophobic Nature Committed through Computer Systems. http://conventions.coe.int/treaty/en/Treaties/Word/189.doc.

Council of Europe. 2007 (Opened for signature on 25 Oct. 2007). Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse. http://www.coe.int/t/dghl/standardsetting/children/Source/Text_en.doc.

Council of Europe.2008. *Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism* (1 May 2008) CETS No. 198. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/198.

Council of Europe. 2009 (Opened for Signature on 18 Jun 2009). Council of Europe Convention on Access to Official Documents. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680084826.

Council of Europe. 2011. Convention on Preventing and Combating Violence Against Women and Domestic Violence. CETS No. 210. http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/210.

Council of Europe.2008. *Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism* (1 May 2008) CETS No. 198. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/198.

Council of the European Union. 2005. Council Framework Decision 2004/68/JHA of 22 December 2003 on combating the sexual exploitation of children and child pornography.

Council of the European Union. 2005. Council Framework Decision 2005/222/JHA of 24 February 2005 on Attacks against Information Systems. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32005F0222&from=EN.

ECOWAS (Economic Community of West African States). 1975. *Treaty of Economic Community of West African States*. http://www.internationaldemocracywatch.org/attachments/351_ecowas%20treaty%20of%201975.pdf.

ECOWAS. 2011 (Done on 19 Aug. 2011). Directive on Fighting Cybercrime within Economic Community of West African States. https://ccdcoe.org/sites/default/files/documents/ECOWAS-110819-FightingCybercrime.pdf.

ECOWAS. Convention A/P.1/7/92 on Mutual Assistance in Criminal Matters. http://documentation.ecowas.int/download/en/legal_documents/protocols/Convention%20on%20Mutual%20Assistance%20in%20Criminal%20Matters.pdf

EU (European Union). 1995. Convention on Simplified Extradition Procedure Member States, Council Act of 10 March 1995, OJ C 78.

EU. 1995. EU Council Resolution of 17 Jan. 1995 on the Law Interception of Telecommunications, OJ C 329. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31996G1104.

EU. 1996. Joint Action of 29 Nov. 1996 Adopted by the Council on the Basis of Article K.3 of the Treaty on European Union, Concerning the Creation and Maintenance of a Directory of Specialized Competences, Skills, and Expertise in the Fight against International Organized Crime, in Order to Facilitate Law Enforcement Cooperation between the Member States of the European Union, 96/747/JHA. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31996F0747

EU. Joint Action of 29 Jun. 1998 Adopted by the Council on the Basis of Article K.3 of the Treaty on European Union, on Good Practice in Mutual Legal Assistance in Criminal Matters, OJ L 191.pp. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31998F0427.

EU. 1999. Draft Council Act Establishing the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, OJ C 251. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A51999AG0902(01).

EU. 1999. Act of the Management Board of Europol of 15 Oct. 1998 Concerning the Rights and Obligations of Liaison Officers, OJ C 026. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31999F0130(08).

EU. 1999. *Act of 12 March 1999 on Adopting the Rules Governing the Transmission of Personal Data by Europol to Third States and Third Bodies,* OJ C 088. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31999F0330.

EU. 2000. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market (also known as "EU Directive on Electronic Commerce"). http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000L0031&from=en.

EU. 2000. "Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union." http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=URISERV:l33108&from=EN

EU. 2006. Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC (also known as "EU Data Retention Directive"). http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF.

EU. 2007. *Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community*. 2007/C 306/01. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3Aai0033.

EU. 2013. Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on Attacks against Information Systems and Replacing Council Framework Decision 2005/222/JHA. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013L0040&from=EN.

League of Arab States. 1994. Arab Charter on Human Rights.

League of Arab States. 2010 (Done on 21 Dec. 2010). Arab Convention on Combating Information Technology Offences. https://cms.unov.org/DocumentRepositoryIndexer/GetDocInOriginalFormat.drsx?DocID=3dbe778b-7b3a-4af0-95ce-a8bbd1ecd6dd.

OAS (Organization of American States). 1969 (Opened for Signature on 22 November 1969). American Convention on Human Rights. https://www.oas.org/dil/treaties_B-32_American_Convention_on_Human_Rights.pdf.

OAS General Assembly. (8 Jun. 2004). *The Inter-American Integral Strategy to Combat Threats to Cyber Security.* AG/RES.2004 (XXXIV-O/04).

OAU (Organization of African Unity). 1991. Abuja Treaty Establishing The African Economic Community. http://www.wipo.int/edocs/lexdocs/treaties/en/aec/trt_aec.pdf.

OAU. 1981. African Charter on Human and Peoples' Rights.

SADC (Southern African Development Community). 2002. "SADC Protocol on Mutual Legal Assistance in Criminal Matters." http://www.sadc.int/files/8413/5292/8366/Protocol_on_Mutual_Legal_Assistance_in_Criminal_Matters_2002.pdf.

SCO (Shanghai Cooperation Organization). 2009 (Done on 16 Jun. 2009). Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security. http://www.ccdcoe.org/sites/default/files/documents/SCO-090616-IISAgreement.pdf.

UN (United Nations). 1966 (Adopted on 10 December 1966). International Covenant on Civil and Political Rights. https://treaties.un.org/doc/Publication/UNTS/Volume%20999/volume-999-I-14668-English.pdf.

UN 2000 (Adopted on 25 May 2000). Optional Protocol to the UN Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography. http://www.ohchr.org/Documents/ProfessionalInterest/crc-sale.pdf.

UN Commission on Human Rights. 1999 (Adopted on 26 April 1999). Resolution 1999/36 on Right to freedom of opinion and expression (E/CN.4/1999/L.52). http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/EN/foraff/142549.pdf.

UN Economic and Social Council. 2011. *Resolution Prevention, Protection and International Cooperation Against the Use of New Information Technologies to Abuse and/or Exploit Children.* E/RES/2011/33. http://www.un.org/en/ecosoc/docs/2011/res%202011.33.pdf.

UN General Assembly. 1990 (Adopted on 14 December 1990). Resolution 45/121 on the Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders (A/RES/45/121). http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/45/121.

UN General Assembly. 1946 (Adopted on 14 December 1946). Resolution 59(I) on the Calling of an International Conference on Freedom of Information [A/RES/59(I)]. http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/59(I).

UN General Assembly. 1948 (Adopted on 10 Dec. 1948). Universal Declaration of Human Rights. http://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/eng.pdf.

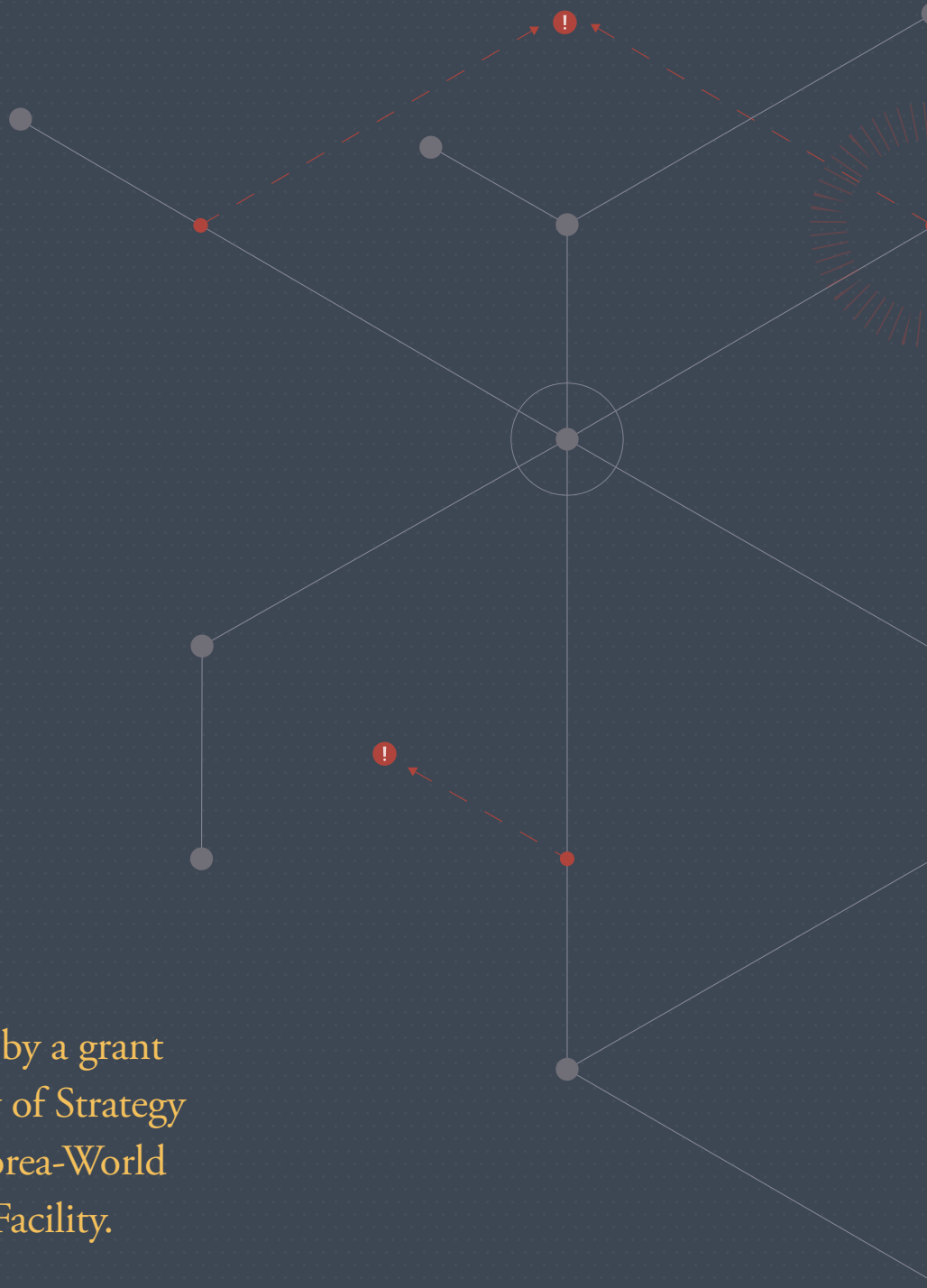
UN General Assembly. 1990. "Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, 68th Plenary Meeting." http://www.un.org/documents/ga/res/45/a45r121.htm.

UN General Assembly. 2000. *United Nations Millennium Declaration.* A/RES/55/2. http://www.un.org/millennium/declaration/ares552e.htm.

UN General Assembly. 2013 (Adopted On 18 December 2013). Resolution 68/167 on the Right to Privacy in the Digital Age (A/RES/68/167). http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/167.

UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression and the ACHPR Special Rapporteur on Freedom of Expression and Access to Information. 2011 (Adopted on 1 Jun. 2011). *International Mechanisms for Promoting Freedom of Expression: Joint Declaration on Freedom of the Media and the Internet.* http://www.osce.org/fom/78309?download=true.

WTO (World Trade Organization). 1994 (Adopted on 15 Apr. 1994). Agreement on Trade-Related Aspects of Intellectual Property Rights. https://www.wto.org/english/docs_e/legal_e/27-trips.pdf.



This Project was financed by a grant from the Korean Ministry of Strategy and Finance under the Korea-World Bank Group Partnership Facility.

The Project team was led by staff of the World Bank, and included the participation of the following organizations: the Council of Europe, the International Association of Penal Law, the International Telecommunication Union, the Korea Supreme Prosecutors Office, the Oxford Cyber-security Capacity Building Centre, the United Nations Conference on Trade & Development, the United Nations Interregional Crime and Justice Research Institute, and the United Nations Office on Drugs & Crime.

THE WORLD BANK
IBRD • IDA | WORLD BANK GROUP

PARTNERS

United Nations