Legal Aspects of Cybersecurity

Artur Appazov

Faculty of Law
University of Copenhagen
2014

Contents

1 Purpose and Scope

The following material is the examination of literature on cybersecurity and cybercrime. Although the following material does not include examination of all existing writing in the area, it includes a number of important sources that are illustrative of the main issues covered in contemporary works on the matters of cybersecurity and cybercrime. The following material is presentation of the main themes and problems as reflected by the literature as a whole without providing separate reviews on specific academic or professional works. Rather, the result of the review is systematization of ideas and concerns as well as existing solutions on the problem of cybercrime and cybersecurity. It is an attempt to organize thinking and current state of academic knowledge on the issues of cybersecurity in its very general form as allowed by the limitations of the projects.

Despite the initial proposal for the material was examination of the literature on cybercrime, the closer analysis revealed that consideration of the issues of cybercrime in separation from a broader concern of cybersecurity would be incomplete and would fail to reflect the entire picture of the problem and risks associates with network technologies. Therefore, in addition to criminal matters the material discusses a wider range of considerations.

The term cybercrime itself, first coined by William Gibson in 1982 and popularized in his novel *Neuromancer*, became a popular descriptor of the "mentally constructed virtual environment within which networked computer activity takes place."[1] This term has come to symbolize the insecurity and risks online, and is generally referred to for description of the general concerns of cybersecurity. These terms are sometimes used interchangeably. Although these concepts have yet to receive clear legal definitions and are to some extent overlapping, in this work the term cybercrime refers to considerations of criminal law and is a subset of the general cybersecurity concept. Cybercrime therefore will be articulated as a component of cybersecurity in light of the general concerns and problems generated by the network and information technologies.

[1] DAVID S. WALL, CYBERCRIME: THE TRANSFORMATION OF CRIME IN THE INFORMATION AGE 10 (Polity Press. 2007).

2 Executive Summary

With the development of information and network technologies and the growing interconnectedness of the world, the risks connected to online communication have become increasingly pressing. Due to the global nature of such communication unhindered by physical boundaries, network technologies challenge the existing international legal structure based on such notions as jurisdiction and sovereignty, where each sovereign jurisdiction regulates communication that takes place in its territory. Online communication, that bypasses geographical and jurisdictional restraints, is a serious concern for the national and international legal orders in their current form.

It is a serious concern in part due to such attributes of online communication as anonymity of the participants of the communication as well as asymmetry of their efforts and the effects that they can achieve. Communication with these attributes operating in the boundless environment of the internet open doors to a wealth of deviation, misuse and crime. Just like the network technology has penetrated virtually every sphere of life on the planet, so did the risks associate with this technology. The crime, facilitated by the network and computer technologies, has become cybercrime; the war, in turn – has turned cyber. Cybercrime, cyberwar and cyberterrorism are among the emerging phenomena that law needs to accommodate. Risks of cyber manifest on various levels – national and transnational (e.g. cybercrime and cyberterrorism) and international (e.g. cyberwar). Collectively, these concerns are describes by the umbrella concept of cybersecurity.

On the national and transnational levels, the matters of cybersecurity primarily concern criminal matters. The main issues are highlighted by the fragmentation of national criminal laws (substantive and procedural) and the need for their harmonization. Diversity of national laws is one of the main reasons of the global cybercrime vulnerabilities, as such diversity does not allow for the development of a single legislative response to the global phenomenon. Many countries, especially developing countries, do not have criminal laws that specifically address cybercrime. Neither do they have adequate capacity to enforce the laws.

On the international level, cybersecurity is concerned with the application of international law to the realities of network and computer technologies, including the possibility of their use in modern warfare. The attribution of the conduct – distinguishing the offender between state or non-state actors – and identification of the offender jurisdiction are significant challenges.

With all these challenges in hand, the effective legal regulation of the internet presumes creation of the viable policy that can adequately address the substance of the problem and its technical complexity on various levels, including legislative interventions in the form of criminalization and harmonization; international cooperation; collaboration with the private sector; professional educational and capacity building in terms of technical support and assistance, especially in the developing countries.

3 General Introductory Remarks

As information technologies become increasingly prevalent, it becomes clear that the global society finds itself in the midst of the communication and technology paradigm shift. It is not the appearance of the new technology as such that defines the state of uniqueness of the current information revolution, as the human society has seen a number of rapid technological advances in the past without quite the same consequences. Rather, it is the unprecedented capability of network and information technologies to enable complex global communication to a degree of unobstructed "one-to-many and many-to-many communication never before seen."[2]

The globally-interconnected digital information and communication infrastructure created by the network technologies touches practically everything and everyone. With billions of people relying on the internet for a wide variety of economic, social, and political interactions, cyberspace "is nothing short of essential to modern life."[3] It is estimated that in just four years from now mobile broadband subscriptions will approach 70 per cent of the world's total population. By the year 2020, the number of networked devices will

[2] JULIE E. MEHAN, CYBERWAR, CYBERTERROR, CYBERCRIME: A GUIDE TO THE ROLE OF STANDARDS IN AN ENVIRONMENT OF CHANGE AND DANGER 9 (IT Governance Publishing. 2008).
[3] Melanie Teplinsky, *Fiddling on the Roof: Recent Developments in Cybersecurity*, 2 AMERICAN UNIVERSITY BUSINESS LAW REVIEW, 227-228 (2013).

outnumber people by six to one, transforming current conceptions of the communication and social interaction.[4]

The internet has brought with it a fundamental change in the way nations and their citizens engage in global economic activity, manage critical infrastructure, and communicate with one another. The hyper-connectivity of the modern world brings a wealth of benefits for governments, enterprises and individuals in that the information exchange is no longer dependent on physical constraints and is available immediately regardless of the distance.

Although the internet is omnipresent in modern society and plays a critical role in many aspects of everyday life, it was never intended to be used by so many and for the vast number of functions it performs today. To the contrary, the internet was designed to allow a small group of scientists to share unclassified reports; it was not designed to transfer sensitive information securely.[5] Moreover, the internet was not designed to allow for easy monitoring of user behavior and was not designed to protect against attacks originating from within the internet itself. That same inherent design persists today, largely unchanged, while the internet's uses have evolved drastically. The ease and anonymity with which people throughout the world can access information systems via the internet, coupled with the internet's inherently flawed design, have created a vulnerability to cyberattacks on an unprecedented scale. Targets of cyberattacks are diverse, and the costs of such attacks are necessarily borne by consumers, private industry, and governments alike. The frequency and sophistication of cyberattacks are likely to increase, as instructions for sophisticated attack methods are made more widely available to would-be attackers via the internet, reducing the technical knowledge required to carry out an attack.[6]

The level of connectivity of the modern world and inherent vulnerabilities of the communication design has become the root of the main challenge – exploitation of vulnerabilities in technological, organizational and legal systems of regulation by all

[4] Comprehensive Study on Cybercrime xvii (John Sandage, et al. eds., United Nations Office on Drugs and Crime 2013).
[5] Howard F. Lipson, Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues 13 (Software Engineering Institute 2002).
[6] William M. Stahl, *The Uncharted Waters of Cyberspace: Applying the Principles of International Maritime Law to the Problem of Cybersecurity*, 40 GEORGIA JOURNAL OF INTERNATIONAL AND COMPARATIVE LAW, 248 (2011).

participants of this communication. This behavior is by no means a novelty in human behavior. However, the possibilities exploiting the vulnerabilities of the network technologies in the context of inter-connected world are significant. These vulnerabilities in the presence of the hyper-connectivity are exploited by all participants of this communication. The participants include criminal enterprises, 'hackers' (whether for financial gain or as a challenge), cause-based groups, proxies for governments, and governments (including their military and intelligence agencies). Motives for the attacks range from financial gain to the advancement of national security interests, to the satisfaction of peer recognition, and to the advancement of various causes.[7]

The actual subject of the debate therefore is not a new type of crime or deviation, but fundamentally reshaped way in which we interact. The academic discourse on the social impact of new technology is nothing new. It is the longstanding concern expressed in the volumes on industrial sociology from Karl Marx to many contemporary commentators.[8] Much like the appearance of the automobile in 1920 created some degree of awe among the socio-legal thinkers, the internet is equally apposite of the new technology today. [9] This new technology created a new level of opportunities where social deviance, including crime, followed. Computer and network related deviance possesses some specificity that creates effects that national and international legal frameworks have never faced before.

Some of the key challenging features of the communication mediated by network and information technologies are:

- **Global Reach**. Network communication does not require any degree of physical proximity. An action in cyberspace is literally borderless and unbounded by such notions as jurisdiction or sovereignly. An instantaneous action is possible between participants who are in different cities, states or countries.[10] Current legal frameworks are traditionally regarded as local in nature, being restricted to the

[7] David Satola & Henry L. Judy, *Towards a Dynamic Approach to Enhancing International Cooperation and Collaboration in Cybersecurity Legal Frameworks: Reflections on the Proceedings of the Workshop on Cybersecurity Legal Issues at the 2010 United Nations Internet Governance Forum* 37 WILLIAM MITCHELL LAW REVIEW, 1748-1749 (2011).
[8] See in e.g. WALL, Cybercrime: The Transformation of Crime in the Information Age 11. 2007.
[9] JONATHAN CLOUGH, PRINCIPLES OF CYBERCRIME 3 (Cambridge University Press. 2010).
[10] Susan W. Brenner, *Toward a Criminal Law for Cyberspace: Distributed Security*, 10 BOSTON UNIVERSITY JOURNAL OF SCIENCE & TECHNOLOGY LAW, 24 - WesLaw paging - (2004).

territorial jurisdiction in which an event occurs. Modern networked technologies have challenged this paradigm requiring significant adjustments to the law.[11]

- **Anonymity**. Cyberspace lets participants conceal or disguise their identities in a way that is not possible in the real world. Anonymity is an obvious advantage of an offender, and digital technology facilitates this in a number of ways. Offenders may deliberately conceal their identity and remove digital evidence by using commercially available encryption software, proxy servers and so on.[12]
- **Asymmetry**. Small participants of the internet communication have more capacity to exercise hard and soft power in cyberspace than in many more traditional domains.[13] Launching a massive cyberattack does not require a large number of people. A single individual with the access to the internet is capable of such an attack due to the possibilities of the network and information technologies. Consequently, a one-to-one scale of commission is not a viable default assumption.[14]

These features seem to be 'incompatible' with the real world jurisdictional fragmentation. Given these challenges that these features introduce, the main question therefore is how to ensure effective monitoring and regulation of user behavior in the integrated global information network in the presence of the current disintegrated legal framework described by a large number of sovereign jurisdictions.

Due to the fact that cyber networks present a unique borderless 'space,' it becomes a lateral, fluid and indivisible single system.[15] As such, physical analogies of space (as our conceptual referent to describe the unfamiliar) are inapposite because cyberspace is not in itself a place; it is an activity, a complex type of mediated communication. In other words, it

[11] CLOUGH, Principles of Cybercrime 7. 2010.
[12] Id. at, 6-7.
[13] Jan-Frederik Kremer & Benedikt Müller, Cyberspace and International Relations: Theory, Prospects and Challenges 45 (Springer 2014).
[14] CLOUGH, Principles of Cybercrime 5. 2010; Brenner, BOSTON UNIVERSITY JOURNAL OF SCIENCE & TECHNOLOGY LAW, 24 - WesLaw paging - (2004).
[15] Brian Nichiporuk & Carl H. Builder, *Societal Implications*, *in* IN ATHENA'S CAMP: PREPARING FOR CONFLICT IN THE INFORMATION AGE (John Arquilla & David Ronfeldt eds., 1997).

is an intricate, multilayered communicative process that is sustained by a series of increasingly complicated technologies.[16]

The asymmetry is displacing hierarchies in every sector of society because hierarchical organization is not an effective means of organizing technologically-mediated activities.[17] Decentralized architecture of the cyberspace equally decentralizes power and authority hierarchy thereby empowering individuals.[18] Due to anonymity, cyberspace has the capacity to create a climate in which the bonds of social conformity are eased, if not eradicated, which further raises the probability of misuse and deviation.[19] The homogeneity of the software used worldwide and decentralized architecture of the internet makes it possible for an individual with a computer linked to the internet to create results for which in real world significant kinetic resources would be necessary.[20] As the information technology permeates all spheres of life, a basic cyberattack is in a way an underlying offence that can be used for the purposes of crime, war or terrorism.

These concerns should play an important role in the ongoing development of information and network technology. Enhancing cybersecurity and protecting critical information infrastructures are essential to each nation's security and economic well-being. Legal regulation of conduct in cyberspace and deterrence of misuse of ICTs must become an integral component of a national cybersecurity and critical information infrastructure protection strategy.

4 Legal Problematics

There are two main challenges that the global interconnectedness and its idiosyncratic features present for the legal systems tailored to regulate the 'real world' behavior. These are the problems that for the sake of convenience can be described as that of jurisdictional

[16] Susan W. Brenner, *The Privacy Privilege: Law Enforcement, Technology and the Constitution*, 7 JOURNAL OF TECHNOLOGY LAW & POLICY, 124-131 (2002).
[17] Susan W. Brenner, *Toward a Criminal Law for Cyberspace: Product Liability and Other Issues*, 5 UNIVERSITY OF PITTSBURGH JOURNAL OF TECHNOLOGY LAW AND POLICY (2005).
[18] Nichiporuk & Builder, Societal Implications. 1997.
[19] Brenner, UNIVERSITY OF PITTSBURGH JOURNAL OF TECHNOLOGY LAW AND POLICY, (2005).
[20] Susan W. Brenner & Joseph Schwerha, *Transnational Evidence-Gathering and Local Prosecution of International Cybercrime*, 20 JOHN MARSHALL JOURNAL OF COMPUTER AND INFORMATION LAW, 347-377 (2002).

fragmentation and that of the attribution of behavior. The following briefly introduces the two major legal problems of the legal regulation of conduct in cyberspace.

4.1 Sovereignty and Jurisdictional Fragmentation

The problem of jurisdictional fragmentation follows from the fact that it does not and cannot agree with the global nature of cyberspace. Jurisdiction, inherently linked to the notion of state sovereignty, imposes an area of exclusive responsibility of a sovereign state over its territory and/or its citizens, thus excluding any extra-jurisdictional involvement of other states. The sovereign equality of states is protected by rules of customary public international law.[21] No state, therefore, can claim sovereignty over cyberspace and thus introduce its effective regulation.[22]

It is one thing to enact laws that regulate conduct, it is quite another to assert jurisdiction over conduct that may be located or originate anywhere in the world. Cyberspace is a distinct phenomenon, beyond traditional rules based on geographical location.[23] Jurisdictional fragmentation, for example, becomes an obstacle when certain online conduct entails criminal responsibility. Normally, when a suspect has allegedly harmed victims or interests in one country, but is located in a second, the law enforcement systems of both countries usually have to cooperate in making both the suspect and evidence of the crime amenable to justice processes. Given the relative ease with which online offenders can commit criminal acts remotely, the law enforcement response to criminal conduct must rely significantly on trans-border mechanisms such as mutual legal assistance and extradition.[24] However, these mechanisms are not always readily available or practicable, partially due to the different legal qualifications of online conduct in various jurisdictions.[25] Specific conduct that is criminally punishable in the country A may not be criminal in the country B. Yet, the alleged offender might be located in the country B creating effect or interfering with information infrastructure in the country A. Moreover, in the case of

[21] Comprehensive Study on Cybercrime 184. 2013.
[22] Michael N. Schmitt, Tallinn Manual on the International Law Applicable to Cyber Warfare 16 (Cambridge University Press 2013).
[23] CLOUGH, Principles of Cybercrime 405. 2010.
[24] Alamie M. Weber, *The Council of Europe's Convention on Cybercrime*, 18 BERKELEY TECHNOLOGY LAW JOURNAL (2014).
[25] Gregor Urbas, *Cybercrime, Jurisdiction and Extradition: The Extended Reach of Cross-Border Law Enforcement*, 16 JOURNAL OF INTERNET LAW, 8 (2012).

cyberspace, it is not easily identifiable whether the threat is originated internally or externally.[26]

While jurisdictional fragmentation does not seem to be an unresolvable problem in highly integrated societies such as the Europe Union, where the laws of each participating jurisdiction to significant degree correspond to each other and coherently regulate similar conduct, this is not the case worldwide. Many developing countries have neither relevant laws that regulate conduct in cyberspace and where necessary introduce responsibility for breaches, nor do these countries have capacity to enforce such laws. In dealing with real world crime, the developed world can ward off the potential threats by strengthening physical border control and introducing strict immigration policies that regulate physical migration. In the case of conduct in cyberspace, there are no such remedies available.

An example is provided by the so called Love Bug malicious software or malware, which made its way around the world's computers in 2001. Originating in the Philippines, the malware infected millions of computers and caused an estimated $10 billion in lost work hours of such businesses as Ford, Siemens, and Microsoft, as well as government departments of various countries.[27] However, prosecution of the author of the code, a graduate student whose thesis proposal on computer viruses had apparently been rejected, proved difficult. At the time, the Philippines had no specific computer crime offenses that matched the dissemination of malicious code, and an attempt to charge credit card offenses instead floundered. Because of this legislative deficiency, the suspect could not be extradited to countries that suffered harm and that had adequate laws for prosecution.[28]

4.2 Attribution: Determining the Responsibility for Harmful Conduct

The legal effects of the conduct in cyberspace can be seen from the perspectives of various participants of online communication – the perspective of an individual (a criminal act, regulated by the national criminal law) and the perspective of a state (an act of aggression regulated by the international law). The asymmetry of the cause-effect relationship in the

[26] SUSAN W. BRENNER, CYBERCRIME AND THE LAW: CHALLENGES, ISSUES, AND OUTCOMES 211 (Northeastern University Press. 2012).
[27] Susan W. Brenner & Bert-Jaap Koops, *Approaches to Cybercrime Jurisdiction*, 4 JOURNAL OF HIGH TECHNOLOGY LAW, 6-7 (2004).
[28] Urbas, JOURNAL OF INTERNET LAW, 8 (2012).

internet does not allow distinguishing with ease between participants standing behind an attack – an individual or a government. Performed by an individual, it is hard to establish whether that individual acted as an agent of a state or on his own. Thus, if a participant engages in the harmful conduct, the applicable law and the consequences of such conduct will depend on whether the participant is a physical person or in fact a government behind the individual. The Tallinn Manual, a comprehensive text on the applicability of the existing international law to cyber warfare, recognizes this problem.[29] As countermeasures can only be lawful if it is for the offending state's conduct, the attribution of conduct is crucially important. A nation must show that a cyberattack qualifies as an 'armed attack' in the context of internationally accepted rules of warfare in order to respond with force, otherwise nations are forced to rely only upon criminal proceedings.[30]

Thus, there are two dimensions of legal effects produces by harmful online conduct – provided that the conduct is criminalized, it will always fall within the ambit of criminal law. However, if the effects of the conduct are serious enough to entail consequences for the national security, such conduct can be seen in the dimension of cyberaggression and the international law.

Victimized nations seeking to take action under the current international legal framework must first determine the source and nature of a cyberattack. In doing so, a nation must equate a cyberattack to either a traditional armed attack, or to a criminal act. Attributing a physical attack perpetrated with traditional weaponry to those responsible involves a two-prong analysis; it is determined whether another nation (as opposed to individuals or other non-state groups) was responsible for the attack, and if not, the attack is addressed as a criminal matter. Historically, the evidence indicating that another nation perpetrated a physical attack, thus constituting an act of war, was relatively clear. An attack involved physical destruction that only another nation had the resources to inflict, and soldiers wearing the uniform of the aggressor nation carried out the attack. The circumstances surrounding most cyberattacks rarely produce such clear evidence. By nature, cyberwarfare represents a disaggregation of combatants and requires significant geographic dispersal of assets where the identity and location of attackers are masked.

[29] Schmitt, Tallinn Manual on the International Law Applicable to Cyber Warfare 29-37. 2013.
[30] Stahl, GEORGIA JOURNAL OF INTERNATIONAL AND COMPARATIVE LAW, 261-262 (2011).

Moreover, nations without sophisticated cyberspace capabilities or those wishing to further disguise the attack's source may contract with for-hire enterprises across the world that are willing to carry out cyberattacks against legitimate' targets. Identifying responsible parties is further complicated by the rapid advancement in computer technology, which creates an almost continuous learning curve that places law enforcement at an extreme disadvantage in their attempts to attribute responsibility for an attack. The technological challenges cyberspace poses, coupled with the problem of asymmetry and anonymity, exponentially increas the complexity of the cross-jurisdictional investigative challenges.[31]

It is common for online attackers to use so called 'slave' computers owned by innocent parties in their assaults. The place from which a cyberattack originated is ambiguous because, while attacks might be routed though internet servers in, for example, China, they might not originate in China. The slave computers can be anywhere in the physical world, because real space is irrelevant to activity in cyberspace.[32] In these circumstances, point of origin of an attack provides little guidance in attributing the conduct.

In the notorious cyberattacks on Iran, Estonia and Georgia,[33] the victimized nations were unable to attribute responsibility for the attack. Each example demonstrates the inherent difficulty of determining responsibility for a cyberattack, the nature of the attack, and the intentions of those responsible. For example, the Estonia attack, which originally appeared to be a state-sponsored cyberattack by Russia, was relatively unsophisticated and well within the capabilities of mere civilians. Such ambiguity surrounding the perpetrators and their intentions is a significant obstacle to any victimized nation's ability to defend itself, and current legal regimes do little to address the problem. The problem, at its core, is evidentiary; a nation under attack must properly attribute the attack before choosing a course of action but rarely has immediate access to the necessary evidence, which is often in a foreign jurisdiction and can be destroyed quickly and easily. Gathering evidence of an attack, which is ephemeral by nature, is further hampered by cross-border law

[31] Id. at.
[32] BRENNER, Cybercrime and the Law: Challenges, Issues, and Outcomes 195. 2012.
[33] See infra at 20-21.

enforcement's reliance on international agreements that were not designed with the unique problems of cyberaggression in mind.[34]

Some literature on the subject offers consideration of the severity of the attack and place of origin as indicative of the state involvement in the harmful online conduct. Thus, Tallinn Manual suggests that if an attack is launched from governmental cyber infrastructure, it might be indicative of governmental involvement. However, such position is somewhat naïve. It is doubtful that any government is reckless enough to launch an cyber operation against another country from its governmental portals when an easier solution would be to use hacking personnel operating from anywhere else but the state infrastructure. After all, as the Manual recognizes, the government computers may have come under control of non-state actors.[35]

5 Cybersecurity as an Umbrella Concept

In general, the literature suggests to distinguishing between various types of cybersecurity concerns. It separates a basic cyberattack into three general categories: cybercrime, cyberterrorism, and cyberwarfare. Cyberespionage is another separate cybersecurity concern connected to either state intelligence or such notion as hacktivism. Dividing cybersecurity into manageable components facilitates the development of national and international law governing the rights and duties of individuals and nations with respect to each category of activity (with the exception of espionage, there are no legal treaties that regulate espionage, separating cyberespionage as notion that falls outside the legal regulation). This approach can help address the shortcomings of present national and international legal frameworks in a more effective manner.[36]

As discussed, cyberattacks often do not closely resemble traditional criminal activity; it is often difficult to establish that the conduct at issue is criminal, as opposed to an act of war or terrorism. In the context of cyberspace, states generate crime and terrorism as well as war, and individuals wage war in addition to committing crimes and carrying out acts of

[34] Stahl, GEORGIA JOURNAL OF INTERNATIONAL AND COMPARATIVE LAW, 260 (2011).
[35] Schmitt, Tallinn Manual on the International Law Applicable to Cyber Warfare 34-35. 2013.
[36] Stahl, GEORGIA JOURNAL OF INTERNATIONAL AND COMPARATIVE LAW, 270 (2011).

terrorism. Cyberattacks largely defy the simple categorization of activity defined by existing laws making it difficult for nations to apply the traditional definitions of crime, terrorism, warfare or espionage as understood under existing law. Traditional classifications of crime, terrorism, and warfare break down due to the aforementioned asymmetric nature of network communication. By giving nonstate actors access to a new, diffuse kind of power, cyberspace erodes states' monopolization of the ability to wage war and effectively levels the playing field between all actors.[37]

The legal and legislative analyses of cybersecurity issues must distinguish not only among different cyberthreat categories enumerated above and actors, such as nation-states, terrorists, criminals, and malicious hackers, but also among different types of cyberthreats. Such cyberthreats include threats to critical infrastructure, which could lead to loss of life or significant damage to our economy; and threats to intellectual property, which could affect a nation's long-term competitiveness.[38]

Concerning critical infrastructure, some commentators believe that at the moment, there is no real likelihood that non-state actors possess the capacity to bring down the banks, transportation systems, electric grid, and communication systems through catastrophic cyberaggression.[39] Wall, for example, attributes the 'popularity' of cybercrime to the media. He posits that the media construction of the cybersecurity imagery is so spectacularly dramatized and the internet is so newsworthy that a single dramatic incident of cybercrime has the power to shape public opinion and fuel public anxiety, frequently resulting in demands for instant and simple solutions to extremely complex situations.[40] However, despite such skepticism, commentators accept that cyberterrorism and cyberwar are a nearing reality. Cybercrime, they warn, is advancing in both volume and sophistication.[41] Modern hackers use increasingly sophisticated methods to attack a variety of targets that occupy nearly every corner of our society: private persons, corporations, religious

[37] Id. at, 261.
[38] Jorge L. Contreras, et al., *Mapping Today's Ceybersecurity Landscape*, 62 AMERICAN UNIVERSITY LAW REVIEW, 1119 (2013).
[39] Brian B. Kelly, *Investing In a Centralized Cybersecurity Infrastructure: Why "Hacktivism" Can And Should Influence Cybersecurity Reform* 92 BOSTON UNIVERSITY LAW REVIEW, 1671-1673 (2012); CLOUGH, Principles of Cybercrime 11. 2010.
[40] WALL, Cybercrime: The Transformation of Crime in the Information Age 14. 2007.
[41] Peter M. Shane, *Cybersecurity: Toward a Meaningful Policy Framework*, 90 TEXAS LAW REVIEW (2012).

institutions, and governmental entities, including local police units, industrial and utility systems, and major governmental agencies and legislative bodies.[42]

Other commentators, such as Kelly and Mehan, are somewhat more alarmist.[43] Consider the following statistics from 2010. The cost of cyberattacks on private citizens worldwide, when accounting for both the direct financial harm and time lost due to recovery after cyberattacks, totaled $388 billion. This figure amounts to more than the global black market for marijuana, cocaine, and heroin combined. Statistics aside, the magnitude of harm posed by a major cyberattack was summarized in 2003 by Richard A. Clarke, former Special Advisor on Cyberspace Security to President George W. Bush, in his testimony before Congress:[44]

> The threat is really very easy to understand. If there are major vulnerabilities in the digital networks that make our country run, then someday, somebody will exploit them in a major way doing great damage to the economy. What could happen? Transportation systems could grind to a halt. Electric power and natural gas systems could malfunction. Manufacturing could freeze. [… E]mergency call centers could jam. Stock, bond, futures, and banking transactions could be jumbled. If that major attack comes at a time when we are at war, it could put our forces at great risk by having their logistics system fail.[45]

With the convergence of today's commercial systems, a coordinated cyberattack against stock markets and banks could erode consumer confidence and effectively create a global financial crisis.[46]

Particularly significant is the observation that the actual, rather than perceived, dangers posed by cyberaggression are not always immediately evident to potential or actual victims. Either they are not individually regarded as serious, or they are genuinely not serious, but possess a latent danger in their aggregation or being precursors to more serious crimes. For example, computer integrity offences often pave the way for other

---

[42] Kelly, BOSTON UNIVERSITY LAW REVIEW, 1671-1673 (2012).
[43] MEHAN, Cyberwar, Cyberterror, Cybercrime: A Guide to the Role of Standards in an Environment of Change and Danger 73. 2008.
[44] Kelly, BOSTON UNIVERSITY LAW REVIEW, 1674-1675 (2012).
[45] Cited in id. at, 1675.
[46] Stahl, GEORGIA JOURNAL OF INTERNATIONAL AND COMPARATIVE LAW, 249 (2011).

forms of more serous offending – identity or information theft from the computer only becomes serious when it is used against the owner (or incitement to violence).[47]

While cybersecurity concerns of non-critical nature do not generate doubts as to their plausibility, the danger to which the critical infrastructure can be exposed is still questionable. In order to demonstrate the true scope of the threat, a sober analysis provided in the literature of the largest cybersecurity incidents in recent time is illustrative.[48]

The SQL Slammer

One of the earliest examples go back to 2003 when at 00:30 (EST) on January 25 a virus that is known as Slammer infected its first computer: a web server running Microsoft's database software SQL. Slammer was designed to replicate itself and send new copies out across the Internet. That simple but efficient design ensured that in just three minutes, by 00:33, the number of infected machines was doubling every 8.5 seconds.[49]

One infected network belonged to Ohio utility company FirstEnergy; it was located in their Davis-Besse nuclear power plant. Slammer snaked its way into the plant's systems via a contractor's unsecured connection and began to slow down the plant's servers due to the constant flow of Slammer copies being flung out across the network. Eventually, two monitoring systems at the plant crashed and were not restored until six hours had passed.[50] The story of Slammer's infection of a nuclear power plant back in 2003 is indicative of the vulnerabilities of the digital systems of control of critical infrastructural objects. However, the consequences of Slammer infection were much less impressive than the fact itself. The plant was offline at the time the infection occurred, and had been so for nearly a year. The failed monitoring system had an analog backup system that was not compromised. Moreover, no disruptions in service or power outages were traced to

[47] WALL, Cybercrime: The Transformation of Crime in the Information Age 209-210. 2007.
[48] Karson K. Thompson, *Not Like an Egyptian: Cybersecurity and the Internet Kill Switch Debate*, 90 TEXAS LAW REVIEW (2011).
[49] Id. at, 470.
[50] Id. at, 471.

Slammer, and the vulnerability that Slammer exploited was so well-known that Microsoft had deployed a patch fixing the problem six months before Slammer was released.[51]

However, the mere fact that the virus did not produce devastating consequences and that the system was protected enough to cope with the infection does not in itself testify for implausibility of such consequences. After all, disruption of the integrity of the monitoring and systems of the nuclear facility might not have been the intention of the author of the virus.

Supervisory Control and Data Acquisition (SCADA) Systems Security and Stuxnet

Supervisory control and data acquisition (SCADA) systems are used to monitor and control critical industrial processes like power generation.[52] A variety of industries across the globe employ some form of SCADA system. SCADA systems were developed in the 1960s, and many systems based in whole or in part on that initial design remain in use today. These technological dinosaurs were never designed to interface with massive corporate intranets that put SCADA systems within reach of the Internet and all its cyber pathogens, such as Stuxnet.[53]

Stuxnet, discovered on July 14, 2010, was described as one of the most sophisticated and unusual pieces of malicious software ever created and was the first worm built not only to spy on industrial systems, but also to reprogram them, and manage their industrial infrastructure.[54] The worm spread like a traditional Windows-based rootkit but was uniquely targeted at specific SCADA subsystems. Though tens of thousands of computers were ultimately infected with Stuxnet, the 'epicenter' of the infection was Iran, where it targeted five Iranian industrial processing organisations. Some security experts speculate that the final target was Iran's Bushehr nuclear power plant, a fear confirmed at least in part by the Iranian government.[55] While Stuxnet did not take control of the nuclear facility, which it was more than capable of doing, the damage it caused delayed the facility's opening by several months. Stuxnet has also been found in other infrastructure systems in

[51] Id. at, 471-472.
[52] CLOUGH, Principles of Cybercrime 11. 2010.
[53] Thompson, TEXAS LAW REVIEW, 472 (2011); CLOUGH, Principles of Cybercrime 11. 2010.
[54] Stahl, GEORGIA JOURNAL OF INTERNATIONAL AND COMPARATIVE LAW, 259 (2011).
[55] Thompson, TEXAS LAW REVIEW, 472-473 (2011).

India, Pakistan, and Indonesia raising concerns that once sophisticated malware is released into a network, it can spread unpredictably.[56]

Though Stuxnet's sophistication and specificity are indeed a cause for concern, once again, the risks were blown out of proportion by the media and their cybersecurity sources.[57] In the aftermath of its detection, experts and media personnel alike were quick in putting the implicative tag of 'act of war' onto the use of the malicious program, although no competent justification for such labeling was offered.[58] Siemens, the manufacturer of the targeted machines, reported that no plant operations had been disrupted as a result of Stuxnet. Further, the Siemens systems used in Iran were modified and illegally acquired, meaning they seemed to lack even the imperfect security measures typical of SCADA systems.[59]

Given the potential military capacity of Stuxnet, the problem of attribution is illustrative. If a hostile nation were able to seize control of a nuclear facility in this manner, a threatened nation would find it difficult to justify retaliation by force under existing international law.[60]

Information Security

Internet-based threats are not only about crippling infrastructure and disabling important systems. Information security is a prime consideration for many web-connected entities. In December 2010, Google was on the receiving end of a cyberattack intended to give the perpetrators access to the Gmail accounts of various Chinese human rights activists. Analysts believe the attackers sent e-mails to Google employees, attaching PDF files containing hidden software that automatically (but discreetly) installed itself when the documents were opened. Once installed, the software gave the attackers the ability to explore some of Google's internal systems.[61]

---

[56] Stahl, GEORGIA JOURNAL OF INTERNATIONAL AND COMPARATIVE LAW, 259 (2011).
[57] Thompson, TEXAS LAW REVIEW, 473-474 (2011).
[58] Sascha Knoepfel, *Clarifying the International Debate on Stuxnet: Arguments for Stuxnet as an Act of War in* CYBERSPACE AND INTERNATIONAL RELATIONS: THEORY, PROSPECTS AND CHALLENGES 117-124, (Jan-Frederik Kremer & Benedikt Müller eds., 2014).
[59] Thompson, TEXAS LAW REVIEW, 473-474 (2011).
[60] Stahl, GEORGIA JOURNAL OF INTERNATIONAL AND COMPARATIVE LAW, 260 (2011).
[61] Thompson, TEXAS LAW REVIEW, 474 (2011).

In March 2011, RSA, the computer-security division of EMC Corporation, was also attacked. The RSA hack took advantage of unwary employees, enticing them to open spreadsheets laced with malicious code. Once inside, the hackers extracted information related to the company's SecurID authentication products, which some forty million businesses use to add another layer of protection to their networks. Though RSA insists the stolen information does not enable a successful direct attack on any of their RSA SecurID customers, the incident does illustrate that no one – not even a security expert – is perfectly safe.[62]

Attacks on Estonia and Georgia

The attack on Estonia represents the best-known example of a coordinated cyberattack on a sovereign nation's critical infrastructure, and it illustrates the need for an international effort to coordinate cybersecurity policy. The attack was debilitating, disrupting government communication support systems, and the online platforms of banks, retailers, and newspapers. The damage inflicted by the attack necessitated a response from the Estonian government; however, the government could do very little in the absence of established procedures for international cooperation because the attacks originated in foreign jurisdictions. The attack demonstrated that the internet is a viable alternative to traditional modes of warfare and terrorism. It also reaffirmed that the absence of a comprehensive international legal framework with the flexibility to cope with the complex nature of cyberspace has hampered efforts to deter such acts and prosecute those responsible.[63]

Estonian public and private sectors suffered a prolonged cyberattack campaign that lasted several weeks. The attack, which occurred in waves over several weeks, disrupted the websites of the Estonian President and Parliament, the vast majority of Estonian ministries, three of the country's six largest news organizations, and two of its major banks. The crippling impact of the attack was due, in part, to the fact that the Estonian government conducts most of its basic operations using the Internet. The prolonged disruption of critical websites caused widespread unrest. Although it is claimed that the attacks

[62] Id. at, 474-475.
[63] Stahl, GEORGIA JOURNAL OF INTERNATIONAL AND COMPARATIVE LAW, 250-251 (2011).

originated within Russian jurisdiction, Estonia was never able to link them directly to the Russian government. However, the speculation that Russian government was behind the attacks led some Estonian officials to advocate for an official request for assistance pursuant to Article V of the North Atlantic Treaty, which requires members of the North Atlantic Treaty Organization (NATO) to assist an ally in the event of an armed attack. Article V expressly states that such assistance may include use of 'armed force' against the aggressor. This marked the first time in NATO history that a member state sought assistance from NATO allies in response to an Internet-based attack on its infrastructure.[64]

Although the Estonian government claims to have proof that the earliest attacks originated from Russian government computers, the nature of a DDoS attack makes determining the original source of the attack difficult. Moreover, hackers who use botnets continue to develop increasingly sophisticated command structures that make the task of tracing an attack to the original source nearly impossible. A subsequent U.S. government investigation found that it is not likely that Russian security agencies were responsible for the attacks, but rather politically driven hackers.[65]

The attack on Georgia in 2008 was designed to disrupt the Georgian government's ability to communicate, demonstrating that a cyberattack can complement traditional armed conflict. The DDoS attack on Georgia began weeks before the armed conflict with Russia, and it overloaded and effectively shut down Georgian servers. A DDoS attack can be enormously effective in disrupting an enemy's ability to coordinate defense measures in preparing for an armed conflict, transmit emergency communications to its citizens, and communicate with the outside world. The attack on Georgia is an example of the crucial role that cyberattacks may play in future instances of armed conflict. Cyberattacks are a cost effective alternative or complement to traditional warfare, as the cost of initiating a cyberattack relative to developing, producing, and using traditional weaponry is nominal. If states can fund an entire cyberwarfare campaign for the cost of replacing a tank tread, it is likely to gain favor as a viable complement or alternative to traditional warfare. The source of the cyberattack on Georgia, as with Estonia, is still the subject of debate. Evidence suggests that a Russian criminal organization was responsible for the attack, but the

[64] Id. at, 256-257; BRENNER, Cybercrime and the Law: Challenges, Issues, and Outcomes 205-208. 2012.
[65] Stahl, GEORGIA JOURNAL OF INTERNATIONAL AND COMPARATIVE LAW, 257-258 (2011).

difficulty in sorting through an attack perpetrated using numerous computers throughout the world makes it impossible to be certain. The lack of consensus on who initiated the attack underscores the challenge of determining who should ultimately be held responsible for initiating a cyberattack.[66]

5.1 Cybercrime and Cybercrime Tools

Computer-related crime is a long-established phenomenon, but the growth of global connectivity is inseparably tied to the development of contemporary cybercrime. Today's cybercrime activities focus on utilizing globalized information communication technology for committing criminal acts with transnational reach.[67] Cybercrime is perhaps one of the more clearly identified thematic areas of cybersecurity and the one where there is almost universal agreement on best practice, as expressed in the Budapest Convention (the Council of Europe Convention on Cybercrime).[68]

The term cybercrime is used to refer both to traditional crimes (e.g., extortion, fraud, forgery, identity theft, and child exploitation) that are committed over electronic networks and information systems as well as to crimes unique to electronic networks (e.g., hacking and denial of service attacks).[69]

'Definitions' of cybercrime mostly depend upon the purpose of using the term. 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

[66] Id. at, 258-259.
[67] Comprehensive Study on Cybercrime 4. 2013.
[68] Satola & Judy, WILLIAM MITCHELL LAW REVIEW, 1753 (2011); Convention on Cybercrime. Council of Europe. (2001).
[69] Teplinsky, AMERICAN UNIVERSITY BUSINESS LAW REVIEW, 249 (2013).

investigative and international cooperation powers, which are better focused on electronic evidence for any crime, rather than a broad, artificial 'cybercrime' construct.[70]

Numerous academic works have attempted to define 'cybercrime.' National and international legislation, however, does not appear concerned with a strict definition of the word. Rather, legislation more commonly referred to 'computer crimes,' 'electronic communications,' 'information technologies,' 'high-tech crime,' 'offence relating to computer information,' 'criminal act of which the target is computer information,' or 'the use of information resources and (or) the impact on them in the informational sphere for illegal purposes.'[71]

It is clear from these approaches that a number of general features could be used to describe cybercrime acts. One approach is to focus on the material offence object – that is, on the person, thing, or value against which the offence is directed.[72] Another approach is to consider whether computer systems or information systems form an integral part of the modus operandi of the offence.[73] Identifying possible cybercrime offence objects and modus operandi does not describe cybercrime acts in their entirety, but it can provide a number of useful general categories into which acts may be broadly classified.[74]

In 2007, Wall suggested three main categories of cybercrime: (i) computer integrity crimes, which are offences relating to the integrity of the computer systems (for example hacking and DDoS); (ii) computer assisted crimes, which are offences assisted by computers (for examples virtual robberies, scams and thefts); and (iii) computer content crimes, which are offences that focus on the content of computers (for example pornography and offensive

[70] Comprehensive Study on Cybercrime xvii. 2013.
[71] Id. at, 11-12.
[72] Francesco Calderoni, *The European Legal Framework on Cybercrime: Striving for an Effective Implementation*, 54 CRIME, LAW AND SOCIAL CHANGE (2010).
[73] Ellen S. Podgor, *International Computer Fraud: A Paradigm for Limiting National Jurisdiction*, 35 U.C. DAVIS LAW REVIEW (2002).
[74] Comprehensive Study on Cybercrime 15. 2013.

communication).[75] UNODC in its 2013 Comprehensive Study on Cybercrime proposes 14 acts that may constitute cybercrime, organized in those same three broad categories:[76]

Acts against the confidentiality, integrity and availability of computer data or systems:

- Illegal access to a computer system
- Illegal access, interception or acquisition of computer data
- Illegal interference with a computer system or computer data
- Production, distribution or possession of computer misuse tools
- Breach of privacy or data protection measures

Computer related acts for personal or financial gain or harm:

- Computer related fraud or forgery
- Computer related identity offences
- Computer related copyright or trademark offences
- Sending or controlling sending of Spam
- Computer related acts causing personal harm
- Computer related solicitation or 'grooming' of children

Computer content related acts:

- Computer related acts involving hate speech
- Computer related production, distribution or possession of child pornography
- Computer related acts in support of terrorism offences

The basic security breach tools with which the enumerated crime are committed are backdoors, botnets, denial-of-service attacks, keyloggers, logic bombs, malware, pharming, phishing, rootkits, smurfing, spoofing, spyware, Trojan horses, viruses, worms, and many more,[77] the reach variety and the definition of which can be found elsewhere.[78]

[75] WALL, Cybercrime: The Transformation of Crime in the Information Age 49-50, 52-129. 2007.
[76] Comprehensive Study on Cybercrime 16. 2013. For substantive elements of each proposed group please refer to the Study at 17-21.
[77] Thompson, TEXAS LAW REVIEW, 469 (2011); BRENNER, Cybercrime and the Law: Challenges, Issues, and Outcomes 36-56, 121-126. 2012.
[78] There are numerous publicly available sources on the technical nature of cybercrime tools. See for example Yvonne Jewkes & Majid Yar, Handbook of Internet Crime (Routledge 2010).

It should be noted that these basic tools are used to commit cyberattacks falling with the categories – cybercrime and cyberaggression (cyber warfare).

Generally, cyberattacks are separated into three major categories: (i) 'automated malicious software delivered over the Internet,' (ii) 'denial-of-service attacks,' and (iii) 'unauthorized remote intrusions into computer systems.'[79] Recent high profile attacks perpetrated against Estonia, Georgia, and Iran[80] have involved a combination of these attack methods, but two types of attack are of particular importance because they are relatively easy to carry out and they are extremely effective. The first type utilizes malware, which was traditionally classified as either a virus or worm. Malware typically infects a computer system through e-mail or when a user visits infected websites, and the nature of its interaction with the system depends on whether it operates like a virus or worm. For example, a virus cannot replicate itself until a user runs the infected program and can lay dormant until that occurs. When it does, the virus replicates itself, infiltrates other programs on the host computer, and modifies them to carry out functions other than those originally intended. Worms, on the other hand, are themselves programs and can replicate independently. Worms can spread within a host computer system and also to any system connected to it by a network or the Internet. As malware has grown more sophisticated it has been further classified by its specific function, common examples of which are Trojan horses, rootkits, sniffers, exploits, bombs, and zombies. Many cyberattacks involve another form of malware that allows multiple computers to be remotely controlled by – or 'slaved' to the commands of – a single operator who can dictate the behavior of those computers. Cyberattackers can effectively magnify the potential devastation caused by an attack by using this slaving technique. This method of attack, used in the 2007 cyberattack on Estonia, allows a cyberattacker to implement a coordinated attack from numerous locations, including within the target network, with very limited warning for a nominal cost.[81]

[79] Mathhew J. Sklerov, *Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect Their Duty to Prevent*, 201 MILITARY LAW REVIEW (2009).
[80] See supra at 20-21.
[81] Stahl, GEORGIA JOURNAL OF INTERNATIONAL AND COMPARATIVE LAW, 254-255 (2011).

The second frequently used method of cyberattack is known as a denial-of-service (DoS) attack. A DoS attack is initiated from a single computer and overwhelms a target computer system with requests until the system can no longer function properly, denying users access to and use of the targeted system. A DOS attack operates by paralyzing the target system's functionality, while malware operates by changing the function the target system is programmed to perform. Both methods capitalize on basic flaws in the Internet's architecture and are often used in conjunction with one another to maximize damage to the target system. The recent cyberattacks on Estonia and Georgia offer vivid examples, as they were carried out using a combination of malware and DoS known as a Distributed Denial of Service (DDoS).[82]

In a DDoS attack, hackers use malware to take control of numerous computers and use the hijacked computers – referred to as 'zombies' – to send a massive series of data packets to the targeted networks. It is particularly difficult to track a DDoS attack to its original source because the owners of the hijacked computers are rarely aware that their systems are being used remotely to carry out a cyberattack. A network of compromised 'zombie' computers is often referred to as a 'botnet.' In 2007, Vint Cerf, widely recognized as one of the fathers of the Internet, estimated that as many as 25% of networked computers worldwide, or 150 million computers, may be part of botnets. Although hackers use other methods in carrying out attacks, malware, DoS, and DDoS used in recent, high profile attacks demonstrates the urgency of addressing cyberattacks and the challenges they pose for victimized nations.[83]

Describing the current cyberthreat landscape, Kellerman addressed the proliferation of targeted attacks, professionalization of cybercrime, automation and commoditization of cyberattack tools, and the evolution of mobile threats, including the explosion in use of mobile malware. Kellerman also identified several recent IT-related trends that challenge our ability to secure cyberspace, such as the migration to cloud computing, the consumerization of IT, the rise of social networking and social media, and the explosion in the use of mobile devices. To address the evolution of the cyberthreat landscape, which

[82] Id. at, 255-256.
[83] Id. at, 256.

urges the development of improved standards for browser security, application security, and e-mail authentication in order to enhance cybersecurity and address cybercrime.[84]

5.2 Hacking and Hacktivism

Early on in the age of the personal computer, manycomputer users performed 'hacks': legal or illegal computer manipulations (e.g., access, defacement, redirects) of computer systems/networks imbued with innovation, style, and technical virtuosity.[85] Hacking activity today involves all types of cyberattacks utilizing the whole range of cybercrime tools. In essence, hacking is an umbrella term that most commonly describes illegal or harmful cyberactivity.

While the problem of hacking is primarily addresses by the criminal law on the level of prohibition of the objective elements of hacking conduct, hacktivism introduces a very distinct mental element to hacking. The term hacktivism describes hacking with a leap of political ideology introduced into the hacking activity. It is also commonly defined as the marriage of political activism and computer hacking. When hacking becomes explicitly political - i.e., becomes hacktivism - it is reframed from technical feats with an implied philosophical underpinning to the explicit pursuit of attention for various issues in order to shift public discourse, raise awareness, and create public pressure.[86]

Hacktivists share a set of beliefs, such as tolerance for legal risk, naming practices, scale of collective action and propensity for multinational cooperation. In engaging in illegal activity, hacktivists frequently form a collective in order to target singular issues rather than merely fragmented pockets of data or code. Yet, despite hacktivists' sense of collectivity behind any particular motive for a hack, individual hacktivist operations are primarily conducted by solo or small-group hackers, with little or no apparent coordination of the overall campaign.[87]

In 2010, WikiLeaks gained notoriety for distributing hundreds of thousands of confidential American diplomatic cables via its website. The controversial leaks made the organization

[84] Contreras, et al., AMERICAN UNIVERSITY LAW REVIEW, 1117 (2013).
[85] Kelly, BOSTON UNIVERSITY LAW REVIEW, 1676-1677 (2012).
[86] Id. at, 1677.
[87] Id. at, 1677-1678.

both famous and infamous, subjecting founder Julian Assange to criticism and criminal investigation.[88]

Meanwhile the WikiLeaks website was struggling to stay connected in the face of multiple DDoS attacks. Fighting fire with fire, WikiLeaks supporters in the online group Anonymous launched Operation Payback, orchestrating DDoS attacks of their own against MasterCard, Visa, and PayPal[89] (for suspending donations to WikiLeaks) and flirted with attacking Amazon (for taking down the WikiLeaks site hosted on its servers).[90]

The group Anonymous is the current embodiment of the idea of hacktivism. There are other examples of the group Anonymous activity. Thus, in April 2011, Sony's PlayStation Network - an online gaming community for the company's top-selling video game console - was the victim of a more intrusive cyberattack. Hackers breached security safeguards to steal data from each of the PlayStation Network's seventy-seven million individual user accounts, including birthdates and credit card numbers. Upon discovering the breach, Sony promptly shut down the PlayStation Network for more than a month in order to conduct a thorough security and damage assessment. Sony estimated that the cyberattack caused approximately $170 million in losses for the company. In the weeks preceding the cyberattack, the hackers alleged to be responsible had taken to the blogosphere to declare war on Sony for its decision to sue a hacker in January 2011 for publishing the PlayStation 3 console code obtained from reverse-engineering the device.[91]

In August 2011, Bay Area Rapid Transit (BART) - the San Francisco Bay Area's public transportation system – shut down cell phone service in its subway tunnels to prevent mobile communication between protestors seeking to halt movement of subway trains. Hackers swiftly denounced BART's action, condemning it as a violation of civil rights, and executed a series of cyberattacks on BART websites as retribution. Simultaneously, the hackers orchestrated a live protest with like-minded Bay Area residents in BART stations, causing the complete closure of two downtown San Francisco subway stations during rush

[88] Thompson, TEXAS LAW REVIEW, 475 (2011).
[89] See also Kelly, BOSTON UNIVERSITY LAW REVIEW, 1665 (2012).
[90] Thompson, TEXAS LAW REVIEW, 475-476 (2011).
[91] Kelly, BOSTON UNIVERSITY LAW REVIEW, 1665-1666 (2012).

hour.[92] Also in 2011, Anonymous also targeted U.S. federal and state government entities. CIA.gov and Senate.gov were the victims of DDoS attacks.

In 2011, Anonymous also began increasingly targeting governments and government entities, giving its cyberattacks an overtly political flavor. This trend began early in the year when a Tunisian marketplace vendor set himself on fire after the dictatorship seized his goods. Anonymous caught wind of the event and after investigating the dictatorship in greater depth, determined the Tunisian government was guilty of widely suppressing its citizens' access to the Internet, or at least portions of the Internet that contained unfavorable (but truthful) stories. Anonymous then conducted cyberattacks against several Tunisian government websites and provided Tunisian citizens with software to circumvent the dictatorship's censorship blocks. Within a month, President Zine El Abidine Ben Ali, the country's dictator, fled after the Arab Spring protests escalated. [93]

On 11 April 2013, Denmark experienced a massive DDoS attack on its country-wide digital identification system NemID, for a few hours crippling the access to all services requiring digital identification, which covers almost all areas of life in Denmark, including online banking, municipal services, taxation and health care systems, real estate and land registration, library services, and many other areas. Earlier same week, the websites of the Danish Local Government Association (Kommunernes Landsforening) and the Danish Social Democrats (Socialdemokraterne) had been subjected to DDoS attacks following the group Anonymous declaration of support of the Danish Union of Teachers (Danmarks Lærerforening) in its dispute with the 'Kommunerne.'[94]

Illustrated by the examples above, Anonymous is not defined as, and does not intend to be defined as, the traditional cast of voiceless, faceless hackers. Rather, Anonymous publicly leads the hacktivism movement, the nonviolent use of illegal or legally ambiguous digital tools in pursuit of political ends. Even under the discrete umbrella of hacktivism, however, Anonymous has a distinct make-up: a decentralized (almost nonexistent) structure,

[92] Id. at, 1666-1667.
[93] Id. at, 1680-1681.
[94] Mads Allingstrup, Danmark under Massivt Cyberangreb. Berlingske (11 April 2013), http://www.b.dk/tech/danmark-under-massivt-cyberangreb-0.

unabashed moralistic/political motivations, and a proclivity to couple online cyberattacks with offline protests.[95]

On its website, Anonymous describes itself as an internet gathering rather than a group. Moreover, Anonymous states that it has a very loose and decentralized command structure that operates on ideas rather than directives.[96] Prior to 2008, Anonymous had been most notable for the spread of harmless, humorous Internet pranks like the 'rickroll' and 'lolcats.'[97] A clash with the Church of Scientology in January 2008 changed that perception, however, shedding light on who (or what) Anonymous is today. The group began a campaign against the Church of Scientology after the Church tried to suppress Internet media outlets' publication of a notorious video of movie star Tom Cruise speaking fanatically (and incoherently) about the religion. What differentiated this Anonymous campaign from its prior attacks was its seriousness and breadth. More than 6000 participating members of the operation, dubbed Project Chanology, donned Guy Fawkes masks and protested in the streets of ninety cities worldwide, spanning North America, Europe, Australia, and New Zealand. Meanwhile, online members raided Scientology websites and prevented the Cruise video from altogether disappearing from the Internet. The Church of Scientology had done nothing to initially provoke Anonymous, but Anonymous members took issue with the Church's litigious history and attempted suppression of free speech on the Internet.[98]

Thus, in the wake of its battle against Scientology, some key characteristics of Anonymous emerged: (i) an unrelenting moral stance on issues and rights, regardless of direct provocation; (ii) a physical presence that accompanies online hacking activity; and (iii) a distinctive brand.[99]

[95] Kelly, BOSTON UNIVERSITY LAW REVIEW, 1667-1668 (2012).
[96] Id. at, 1678.
[97] Id. at, 1679.
[98] Id. at, 1679-1680.
[99] Id. at, 1680.

5.3 Cyberwar and Cyberterrorism

Wars are fought within the context of their age with the weapons determined by the prevalent technology of the age.[100] At that, concepts like electronic warfare, information warfare, network warfare, cyberwar and cyberterrorism have been offered to explain the emerging area of conflict. Unlike kinetic weaponry, such as weapons of mass destruction, that cause numerous casualties instantaneously, cyber warfare creates disruptive rather than destructive effects with no less serious consequences.[101]

The term cyberwar refers to actions by a nation-state to penetrate another nation's computers or networks for the purposes causing damage or disruption. It is believed that the world's largest militaries are building cyberwarfare programs, with several nation-states – including the U.S., China, Russia, Israel, and Iran – already considered to have joined the ranks of the cyberwar-capable. These potential military or terrorist threats are, inter alia, the effects of cyberattacks (i) on the power grid could lead to cascading failures across the nation with catastrophic consequences; (ii) on financial systems could lead to economic panic and/or a crashing stock market; (iii) on water systems could open dams causing flooding or make entire cities uninhabitable; (iv) on rail systems (e.g., involving intentional misrouting of trains) could cause massive collisions; (v) on air-traffic control systems could lead to mass casualties; and (vi) on nuclear facilities could result in a nuclear reactor meltdown, leading to catastrophic loss of life.[102]

As already discussed, some experts have suggested that cyberwar concerns have been greatly exaggerated. A recent Dartmouth study of cyberwar funded by DHS concluded that the degree of damage that could be caused in a cyberattack bears no resemblance to an electronic 'Pearl Harbor, although inflicting significant economic costs on the public and private sectors and impairing performance of key infrastructures (via IT networks linked to embedded computer systems, for example) seem both plausible and realistic. Prominent cybersecurity expert James Lewis at the Center for Strategic and International Studies has

[100] MEHAN, Cyberwar, Cyberterror, Cybercrime: A Guide to the Role of Standards in an Environment of Change and Danger 21. 2008.
[101] Craig B. Greathouse, *Cyber War and Strategic Thought: Do the Classic Theorists Still Matter?*, *in* CYBERSPACE AND INTERNATIONAL RELATIONS: THEORY, PROSPECTS AND CHALLENGES 23, (Jan-Frederik Kremer & Benedikt Müller eds., 2014).
[102] Teplinsky, AMERICAN UNIVERSITY BUSINESS LAW REVIEW, 265-267 (2013).

repeatedly expressed skepticism of the view that cyberattacks are likely to cause widespread death, damage, and destruction.[103]

Cyberattacks are not very destructive, compared to kinetic weapons, particularly strategic weapons. It seems fair to say that at this time, the possibility of damage, death and destruction from cyberattack is low. Cyber weapons will have difficulty producing casualties. While acknowledging the gravity of the cyber threat, intelligence officials dramatically toned down their cyberwar rhetoric in early 2013. For example, while Director of National Intelligence James Clapper told Congress in March 2013 that cyberattacks are the most dangerous threat facing the United States, he also said that the intelligence community sees only a remote chance of a major computer attack on the United States in the next two years. Rhetoric aside, experts are struggling to identify appropriate responses to nation-state cyberattacks.[104]

The U.S. military formally distinguishes between two types of offensive cyberpower available to nation-states: Cyber Network Exploitation (CNE) and Cyber Network Attack (CNA). While CNE is essentially espionage, CNA refers to destructive attacks. Specifically, CNAs are defined as actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks or the computers and networks themselves.[105]

As with any traditional forms of war, there are different levels of intensity of cyberwar. Not all of these types of attacks are going to be directed towards destruction of resources or misdirection during an attack. Some will engage in military destructive or disruptive activities, some – in intelligence gathering constituting cyberespionage.[106]

Although creating a typology of cyber operations is difficult due to the nature of the technology involved,[107] Mehan suggests the following calcification of the cyberwar: Class I cyberwar is concerned with the protection of personal information or personal privacy. While the results can still be devastating, Class I cyberwar is considered to be the lowest

[103] Id. at, 273.
[104] Id. at, 274.
[105] Id. at, 267-268.
[106] Greathouse, Cyber War and Strategic Thought: Do the Classic Theorists Still Matter? 24. 2014.
[107] See Kremer & Müller, Cyberspace and International Relations: Theory, Prospects and Challenges. 2014.

grade. Class II cyberwar concerns itself with industrial and economic espionage, which can be directed against nations, corporations or other organizational structures. Class III cyberwar is about global war and terrorism, which includes cyberterrorism, but which may also include attacks against other parts of the critical infrastructure. Finally, Class IV cyberwar is the combination of the techniques of Classes I – III in combination with kinetic military activities.[108]

As for the cyber weaponry itself, it includes all those basic cyber technics that we can find in cybercrime, that is viruses, malware, denial of service, spying, jamming, blocking and so on.[109] The factors that distinguish cyberwar from cybercrime are the object and the level of intensity of the attack and sophistication of the strategy of the attack.

An interesting and rather alarming development is that in November of 2011, the U.S. Department of Defense concluded for the first time that cyberattacks can constitute an act of war to which the United States may respond using traditional military force (i.e., a kinetic, rather than cyber-based, response).[110]

5.4 Cyberespionage – the Advanced Persistent Threat

Cyberespionage refers to state-sponsored theft of industrial and defense secrets and/or intellectual property.[111] The state sponsored cyberespionage poses a serious threat to the economic and national security. Military secrets and valuable corporate intellectual property undermine the long-term competitiveness of the targeted countries.[112]

Some prominent examples of cyberespionage include: Moonlight Maze (1998); Byzantine Hades (2002); Operation Titan Rain (2003); Operation Buckshot Yankee (2008); Operation Night Dragon (2008-2011); Operation Aurora (2009); penetration of Lockheed Martin, BAE Systems and Northrop Grumman (2009); Operation Shady RAT (2006); GhostNet (2009);

[108] MEHAN, Cyberwar, Cyberterror, Cybercrime: A Guide to the Role of Standards in an Environment of Change and Danger 28. 2008.
[109] See Jewkes & Yar, Handbook of Internet Crime. 2010.
[110] Teplinsky, AMERICAN UNIVERSITY BUSINESS LAW REVIEW, 268-269 (2013).
[111] Id. at, 252.
[112] Contreras, et al., AMERICAN UNIVERSITY LAW REVIEW, 1114-1115 (2013).

the RSA Breach (2011); and twenty-three natural gas pipeline operators (December 2011-June 2012).[113]

By some reports, cyberespionage is estimated to cost the United States alone (in terms of lost jobs, innovation, and national security) and its corporations (in terms of lost intellectual property, remediation, and reduced consumer confidence) up toillion annually, but reliably quantifying the potentially staggering costs of cyberespionage has been an elusive goal. Obstacles include the fact that many companies do not know that they have been victimized and even those that do know are often reluctant to disclose out of concern for their reputation.[114]

One particularly insidious form of cyberespionage is known as an advanced persistent threat (APT). APTs are highly targeted malware-based attacks with several distinguishing features. First, as their name suggests, APTs are often advanced. In many cases, they utilize the full spectrum of computer intrusion technologies and techniques and combine multiple attack methodologies and tools in order to reach and compromise their target. Second, APTs are persistent. APT operators seek long-term access to their targets, with attack objectives generally extending beyond immediate financial gain. In order to maintain long-term access to targets, APTs generally operate stealthily for as long as possible. Finally, APTs rely on skilled, motivated, organized and well-funded operators to coordinate and execute attacks. The substantial resources required to operate APTs generally makes them a tool of nation-states. At their essence, APTs are computer intrusions staged by threat actors that aggressively pursue and compromise specific targets, often leveraging social engineering or the 'art of manipulation,' in order to maintain a persistent presence within the victim's network so that they can move laterally and extract sensitive information.[115]

6 Legal Solutions and Strategies

While a viable cybersecurity policy includes a wide range of considerations, legal measures play a key role in the prevention and combating of cybercrime. These are required in all

[113] Teplinsky, AMERICAN UNIVERSITY BUSINESS LAW REVIEW, 253-255 (2013).
[114] Id. at, 256.
[115] Id. at, 256-257.

areas, including criminalization, procedural powers, jurisdiction, international cooperation, and internet service provider responsibility and liability. In particular, at the national level, cybercrime laws most often concern criminalization – establishing specialized offences for core cybercrime acts. Countries increasingly recognize the need, however, for legislation in other areas.[116]

The technological developments associated with cybersecurity and cybercrime mean that – while traditional laws can be applied to some extent – legislation must also grapple with new concepts and objects, such as intangible 'computer data,' not traditionally addressed by law. In many states, laws on technical developments date back to the 19th century. These laws were, and to a great extent, still are, focused on physical objects – around which the daily life of industrial society revolved. For this reason, many traditional general laws do not take into account the particularities of information and information technology that are associated with cybercrime and crimes generating electronic evidence. These acts are largely characterized by new intangible objects, such as data or information.[117]

While criminal law is often perceived as being most relevant when it comes to cybercrime, the legal responses to wider concerns of cybersecurity also include the use of other branches of law, such as civil law and administrative law. Further divisions within these legal regimes include substantive and procedural law, as well as regulatory and constitutional, or rights-based, laws. In many legal systems, each of these regimes are characterized by specific aims, institutions, and safeguards. Cybercrime laws are most usually found within the areas of substantive and procedural criminal law. However, a number of other areas of law are also important.[118]

The matter of criminalization of undesirable conduct in the internet has a two-fold effect: (i) creation of the legal basis for retributive suppression of the conduct, and (ii) creation of a climate of social unacceptability of cybercrime, de-romanticizing and stigmatizing such conduct. Those who use internet to commit crimes grew up with and were socialized by a climate in which the predominating mode of unlawful activity was real-world crime, in its

[116] Comprehensive Study on Cybercrime xviii, 51. 2013.
[117] Id. at, 51.
[118] Id. at, 52.

traditional guises,[119] whereas hacking, for example, does not invoke a feeling of social unacceptability. Rather, it is marked by the ethos of sport almost. Currently, hacking behavior is characterized by a laissez-faire attitude toward liability and legality in many jurisdictions globally..[120] In this sense, conceptualization of cybercrime as a crime proper advances both retribution and deterrence.

6.1 Criminalization

At the national level, both existing and new (or planned), cybercrime laws most often concern criminalization, indicating a predominant focus on establishing specialized offences for core cybercrime acts. Globally, many jurisdictions tend to perceive their criminal and procedural law frameworks to be sufficient, although this masks large regional differences.[121] While many countries in Europe tend to consider their legislation sufficient, the picture is reversed in Africa, the Americas, Asia and Oceania, where more countries view laws as only partly sufficient, or not sufficient at all.[122]

Also, while high-level consensus exists regarding broad areas of criminalization, the detailed provisions reveal more divergent approaches. Thus, offences involving illegal access to computer systems and data differ with respect to the object of the offence (data, system, or information), and regarding the criminalization of 'mere' access as an inchoate crime or the requirement for further intent, such as to cause loss or damage. The requisite intent for an offence also differs in approaches to criminalization of interference with computer systems or data. Most countries require the interference to be intentional, while others include reckless interference.[123] For interference with computer data, the conduct constituting interference ranges from damaging or deleting, to altering, suppressing, inputting or transmitting data. Criminalization of illegal interception differs by virtue of whether the offence is restricted to non-public data transmissions or not, and concerning whether the crime is restricted to interception by technical means. Not all countries criminalize computer misuse tools. For those that do, differences arise regarding whether

[119] Susan W. Brenner, *Toward a Criminal Law for Cyberspace: a New Model of Law Enforcement?*, 30 RUTGERS COMPUTER AND TECHNOLOGY LAW JOURNAL, 39 (2004).
[120] Kelly, BOSTON UNIVERSITY LAW REVIEW, 1693-1694 (2012).
[121] Comprehensive Study on Cybercrime xviii. 2013.
[122] Id. at.
[123] Id. at, xx.

the offence covers possession, dissemination, or use of software (such as malware) and/or computer access codes (such as victim passwords). From the perspective of international cooperation, such differences may have an impact upon findings of dual-criminality between countries.[124]

6.2 Hacktivism and Criminalization

Some commentators propose that targeting hacktivism (as opposed to hacking) in criminalization efforts will most obviously minimize a threshold problem in the larger cybersecurity debate.[125] Perhaps the problem is that criminalization of hacktivism is too complex a legal issue involving specific intent to promote, inter alia, political goals. Also, it might also be challenging from the perspective of social acceptability of such crime. The examples of the Anonymous and Anonymous-led cyberattacks discussed above are illustrative precisely because of the 'Robin Hood' flavor of the Anonymous intent. Just as the mafia was once singled out as the face of organized crime, governmental authorities should capitalize on Anonymous's visibility when discussing cybersecurity with the general public. This singling-out of Anonymous would not be unwarranted. According to a 2012 report published by Verizon, hacktivists (generally) overtook cybercriminals as the group responsible for the largest amount of damage resulting from cyberattacks in absolute dollar figures. Moreover, Anonymous specifically has high public recognition due its reliance on social media (Twitter feeds, YouTube pages, and websites), branding mechanisms (iconic Guy Fawkes masks and naming practices), and politically-charged viewpoints in the course of conducting cyberattacks on highprofile victims. Undoubtedly, sizable sectors of the American public followed or were affected by the PayPal/Visa/MasterCard cyberattacks, the Sony outage, and the Occupy Movement protests.[126]

On the other hand, hacktivism is an umbrella term that covers a number of acts that rather than being a unique activity as such. This is at least true for the objective elements. Some of these acts are already criminalized in various jurisdictions. These acts constitute such crimes as, for example, illegal access to, interception and interference with computer

[124] Id. at.
[125] Kelly, BOSTON UNIVERSITY LAW REVIEW, 1706 (2012).
[126] Id. at, 1706-1707.

data.[127] Hacktivism, however, may differ in its subjective element, that is the specific intent to achieve a specific goal or result.

6.3 Procedure and Evidence

The trans-border nature of cybercrime and the commission of a cybercrime in an electronic environment are the main difficulties that the law enforcement faces. The traditional assumptions about a perpetrator's being observed preparing for, committing or fleeing from an offense no longer hold true.[128] Challenges in the investigation of cybercrime arise from criminal innovations by offenders, difficulties in accessing electronic evidence, and from internal resource, capacity and logistical limitations. Suspects frequently use anonymization and obfuscation technologies, and new techniques quickly make their way to a broad criminal audience through online crime markets.[129]

Identifying a perpetrator, investigating and gathering evidence of the crime can be difficult for various reasons. In addition to the anonymization and obfuscation challenges, the country that hosts the cybercriminal and his activities may not define what is done as illegal and may therefore be unable to prosecute him or cooperate in his being extradited for prosecution elsewhere; the host nation may not have agreements in effect with the victim nation which obligate it to assist in gathering evidence that can be used against the perpetrator; or extremely volatile electronic evidence may have been destroyed, advertently or because it was routine transactional data that was not retained by the Internet Service Provider which the offender used to commit the crime. Cyberspace makes physical space irrelevant. It becomes as easy to victimize someone who is halfway around the world as it is the next-door neighbor.[130]

Therefore, on the procedural level, the main problem for the national law enforcement is reconciliation of the historical fact that police is operationally and organizationally

[127] BRENNER, Cybercrime and the Law: Challenges, Issues, and Outcomes 21. 2012; Comprehensive Study on Cybercrime 78. 2013.
[128] Brenner, RUTGERS COMPUTER AND TECHNOLOGY LAW JOURNAL, 30 (2004).
[129] Comprehensive Study on Cybercrime xxi-xxii. 2013; BRENNER, Cybercrime and the Law: Challenges, Issues, and Outcomes 138-144. 2012.
[130] Brenner, RUTGERS COMPUTER AND TECHNOLOGY LAW JOURNAL, 32-35 (2004).

localized within the boundaries of a jurisdiction (inherently linked to state sovereignty), whereas cybersecurity and cybercrime are globalized and jurisdiction-disturbed.[131]

Law enforcement cybercrime investigations require an amalgamation of traditional and new policing techniques. While some investigative actions can be achieved with traditional powers, many procedural provisions do not translate well from a spatial, object-oriented approach to one involving electronic data storage and real-time data flows.[132]

Evidence is the means by which facts relevant to the guilt or innocence of an individual at trial are established. Electronic evidence is all such material that exists in electronic, or digital, form. It can be stored or transient. It can exist in the form of computer files, transmissions, logs, metadata, or network data. Digital forensics is concerned with recovering – often volatile and easily contaminated – information that may have evidential value. Forensics techniques include the creation of 'bit-for-bit' copies of stored and deleted information in order to ensure that the original information is not changed, and cryptographic file 'hashes,' or digital signatures, that can demonstrate changes in information. This means that sufficient numbers of forensic examiners, availability of forensics tools, and backlogs are required on the part of the law enforcement due to overwhelming quantities of data for analysis. Suspects make use of encryption, rendering access to this type of evidence difficult and time-consuming without the decryption key. In most countries, the task of analyzing electronic evidence lies with law enforcement authorities.[133]

An additional challenge is usage of the technology on the part of the law enforcement – at the moment, cyber offenders seem to better utilize the technological capabilities that they have. The presence of a relevant body of the special knowledge and expertise within the police force is the crucial element in effective regulation of cyberspace.[134] Prosecutors must view and understand electronic evidence in order to build a case at trial. Many developing countries globally do not have sufficient resources for prosecutors to do so. Prosecution computer skills are typically lower than those of investigators. The same holds true for the

[131] WALL, Cybercrime: The Transformation of Crime in the Information Age 160. 2007.
[132] Comprehensive Study on Cybercrime xxii. 2013.
[133] Id. at, xxiii-xxiv.
[134] WALL, Cybercrime: The Transformation of Crime in the Information Age 160. 2007.

judges handling highly specialized cybercrime cases. Judicial training on cybercrime law, evidence collection, and basic and advanced computer knowledge represents a particular priority.[135]

Many jurisdictions do not make a legal distinction between electronic evidence and physical evidence.[136] While approaches vary, many countries consider this good practice, as it ensures fair admissibility alongside all other types of evidence. A number of countries outside of Europe do not admit electronic evidence at all, making the prosecution of cybercrime, and any other crime evidenced by electronic information, unfeasible. While countries do not, in general, have separate evidentiary rules for electronic evidence, a number of countries referred to principles such as: the best evidence rule, the relevance of evidence, the hearsay rule, authenticity, and integrity, all of which may have particular application to electronic evidence.[137]

6.4 Harmonization of Laws

Many countries have elements of the legal enabling environment addressing cybersecurity and cybercrime, but these national legal frameworks vary widely in terms of the manner in which these issues are addressed.[138] In today's globalized world, the law consists of a multitude of national, regional and international legal systems. Interactions between these systems occur at multiple levels. As a result, provisions sometimes contradict each other, leading to collisions of law, or fail to overlap sufficiently, leaving jurisdictional gaps. These differences between national laws lead to the question of whether, and if so, how far, national legal differences in cybercrime laws can and should be reduced. In other words, how important is it to harmonize cybercrime laws? This can be undertaken in a number of ways, including through both binding and non-binding international or regional initiatives. The basis of harmonization may be a single national approach (with all others revising their laws in line), or, more often, common legal elements identified in the law of a number

[135] Comprehensive Study on Cybercrime xxiii-xxiv. 2013.
[136] BRENNER, Cybercrime and the Law: Challenges, Issues, and Outcomes 127-138. 2012.
[137] Comprehensive Study on Cybercrime xxiv. 2013.
[138] Satola & Judy, WILLIAM MITCHELL LAW REVIEW, 1758 (2011).

of states, or expressed within a multilateral instrument – such as a treaty or non-binding international standard.[139]

One of the main arguments in favor of unification of laws across jurisdictions is to avoid safe havens and penalty havens for perpetrators. Thus, if harmful acts involving the internet are criminalized, for example, in State A, but not in State B, a perpetrator in State B can be free to target victims in State A via the internet. In such cases, State A cannot, on its own, effectively protect against effects from such transnational activities. Even where its criminal law allows the assertion of jurisdiction over the perpetrator in State B, it will still require consent or assistance from State B – either regarding the gathering of evidence, or the extradition of the identified perpetrator. In order to protect persons within its own jurisdiction, State B is unlikely to assist where the conduct is not also criminalized in its own country.[140]

Harmonization can also allow for global evidence collection. The harmonization of procedural law is a second indispensable requirement for effective international cooperation. In the above example, if State B does not have the necessary procedural power for expedited preservation of computer data, for instance, then State A will not be able to request this facility through mutual legal assistance. In other words, a requested state can only provide assistance within its territory, to the extent that it could do so for an equivalent national investigation.[141]

6.5 Incident Reporting and Information Sharing

Because of the difficulties arising when trying to define and identify cybercrime, nationally and cross-nationally comparative statistics on cybercrime are much rarer than for other crime types.[142] The measures that might be wanting are those that would improve transparency through obliging individual and corporate victims, under certain circumstances, disclose data breaches.[143]

---

[139] Comprehensive Study on Cybercrime 56-58. 2013.
[140] Id. at, 60.
[141] Id. at, 61.
[142] Id. at, 6; CLOUGH, Principles of Cybercrime 13-14. 2010.
[143] Teplinsky, AMERICAN UNIVERSITY BUSINESS LAW REVIEW, 276-278 (2013).

Cybercrime acts most frequently come to the attention of law enforcement authorities through reports by individual or corporate victims. The UNDOC study provides that 80 per cent of individual victims of core cybercrime do not report the crime to the police.[144] Underreporting derives from a lack of awareness of victimization and of reporting mechanisms, victim shame and embarrassment, and perceived reputation risks for corporations. It is important to highlight initiatives for increasing reporting, including online and hotline reporting systems, public awareness campaigns, private sector liaison, and enhanced police outreach and information sharing. An incident-driven response to cybercrime accompanied by medium and long-term tactical investigations can successfully identify the crime markets and criminal scheme architects, which means a better understanding of the area in need of regulation.[145]

Until the law enforcement has a cumulative picture of victims of cybercrime and their offenders, confusion will remain as to who they are (whether they are physical persons or corporation or governments), the manner of their victimization, and the amount of policing resources that should be allocated to the problem. The inability to construct the offender profile leads to inability to isolate offender motivation for the purposes of criminalization, for example.[146] Reliable information about cybercrime informs policy, practice, and the public. It helps to prevent information sources from over-representing their own interest and it reconciles the needs of the state and interests of other stake-holders, rather than dividing them. Reliable information helps shape public expectations more realistically.[147]

6.6 Institutional Arrangements for Cybersecurity Bureaucracy

The institutional arrangements supporting cybersecurity are as varied and diverse as the approaches to the issues. First, there is no one-size-fits-all response to effective institutional design as globally institutional arrangements vary dramatically. Second, not all cybersecurity issues have a specific institutional dimension. The most obvious one is the

[144] Comprehensive Study on Cybercrime xxi. 2013.
[145] Id. at.
[146] WALL, Cybercrime: The Transformation of Crime in the Information Age 19-21. 2007.
[147] Id. at, 28.

area of cybercrime, where practice indicates that issues of cybercrime, once passed into legislation, are usually within the purview of the law enforcement and the judiciary.[148]

In terms of privacy, for example, a number of examples demonstrate the wide practice of institutional responses:

In the E.U., generally, each country has a Data Protection Agency (DPA) principally responsible for the interpretation and enforcement of data privacy violations. Each DPA is typically an independent agency, with the authority to enforce against other government entities. For those E.U. member states with a criminal component to data protection legislation, national or regional prosecutors may be engaged by the DPA for particular matters. In addition, at the E.U. level, there is a Working Party on Data Protection that determines which countries are compliant with the Directives.[149]

In Argentina, the National Data Protection Directorate (NDPD) established under the Personal Data Protection Act is responsible for digital data protection. The NDPD is under the Ministry of Justice and Human Rights.[150]

In Canada, at the federal level, the Personal Information Protection and Electronic Documents Act (PIPEDA) assigns its oversight and enforcement role to the Office of the Privacy Commissioner of Canada (OPC) which reports to Parliament.[151]

In Malaysia, processing of personal data is regulated by the Personal Data Protection Act 2009 (PDPA). The Personal Data Protection Commissioner is appointed by the Ministry of Information, Culture, and Communications and is in charge of implementing and enforcing the personal data protection laws in Malaysia.[152]

[148] Satola & Judy, WILLIAM MITCHELL LAW REVIEW, 1781 (2011).
[149] Id. at, 1782-1783.
[150] Id. at.
[151] Id. at.
[152] Id. at.

In South Africa, the Protection of Personal Information Act (PPIA) requires that personal information may only be processed by a responsible party that has notified the information Protection Regulator (Regulator), which reports to the President of South Africa.[153]

Strong governmental involvement and institutional solutions in securing cyberspace are justified due to the heavy dependence of the government on technology and cyberspace for its own operations. In addition, government has a unique vantage point from which to observe and understand global economic, political, and technological forces that could give rise to cyberthreats.[154]

On the international level, if members of the international community were able to develop a convention mandating international cooperation on cybersecurity and applying universal jurisdiction to acts of cyberaggression, the benefits would be palpable. One such benefit would an opportunity to create a UN agency comparable to the International Maritime Organization (IMO) whose purpose would be to ensure the safety and security of the internet.[155]

The IMO was created pursuant to the adoption of the Convention on the International Maritime Organization. The purpose of the IMO is to facilitate cooperation among governments in order to ensure that the highest practicable standards in matters concerning maritime safety are in place. The IMO also maintains detailed records of all incidents of piracy, which supports the IMO's policy recommendations and efforts to develop new law when the need arises. The IMO's strategy consists of compilation and distribution of periodical statistical reports, piracy seminars and field assessment missions to regions affected by piracy and the preparation of a code of practice for the investigation and prosecution of the crime of piracy. An agency similar in function to the IMO dedicated to tracking incidents of cyberaggression and fostering cooperation between member nations would help to consolidate the international effort to monitor and deter

[153] Id. at.
[154] Contreras, et al., AMERICAN UNIVERSITY LAW REVIEW, 1123 (2013).
[155] Stahl, GEORGIA JOURNAL OF INTERNATIONAL AND COMPARATIVE LAW, 270-271 (2011).

cyberaggression. Moreover, such an agency would help to legitimize the international legal regime that created it, and would provide sound policy rooted in empirical evidence.[156]

6.7 Personnel Recruitment and Educational Training

There is a need for many governments to broaden cybersecurity personnel recruitment and educational training efforts (in particular for law enforcement, judiciary and other authorities). The US government, for example, established the National Institute for Cybersecurity Education (NICE). NICE together with the Department of Education, and other agencies launched a four-prong strategy to build a cyber savvy nation through training, awareness, through post-graduate educational programs, and professional development for federal security professionals. To meet that goal, NICE targeted a wide array of the population as prospective employees: students and private sector partners.[157]

Any cybersecurity reform legislation should make these arrangements permanent. Governmental agencies should be given the authority and resources to initiate new recruitment and education campaigns and extend the scope of existing ones. The rationale for this investment is two-fold. First, in a world of ever-increasing connectivity, more cybersecurity will be needed to manage that connectivity, so there will be a parallel increase in demand for cybersecurity jobs. Second, through enhancing its presence in recruitment and education, the federal government can attract those individuals to fill cybersecurity jobs who might otherwise have joined the ranks of Anonymous or other hacker groups. Granted, persons who are anti-government or even apathetic towards government may not be persuaded by the government's recruitment efforts. But for those young people who exhibit exceptional computer skills and seek a community that utilizes and appreciates those skills, the recruitment and education campaigns will certainly aid governments in this mission.[158] While not all hacktivists are young, many of them are, suggesting that they might be subject to ideological capture. Without a substantial recruitment effort by governments, there is an obvious lack of an alternative hacking 'career path,' so to speak, for those young persons looking for an outlet for their computer

[156] Id. at, 271.
[157] Kelly, BOSTON UNIVERSITY LAW REVIEW, 1695 (2012).
[158] Id. at, 1696.

skills. Additionally, increased recruitment efforts might even help persuade those who already have joined hacktivist endeavors to work for governments.[159]

7 Technical Solutions

There are two basic technical strategies for critical systems protection – (i) defending the system from the internet risks while the system stays online, and (ii) air gapping the system and the general networks, that is a disconnection of such critical systems from the internet entirely by the authorities.[160] Such proposals have recently been popular with some politicians in light of the developments with the US National Security Agency leaks.

7.1 Defense and Monitoring Systems

The US government partially guards its computers and networks with an intrusion detection system nicknamed 'Einstein.' The Einstein software is designed to conduct real-time surveillance on, make threat-based decisions on, and provide an intrusion prevention system for any activity taking place in certain government computer networks. In performing these functions, Einstein shares information and cooperates with the Department of Homeland Security and the National Security Agency. Thus, currently within its own network, the US government closely coordinates among departments, wipes personally identifiable information from shared cybersecurity data, and operates on a real-time response basis.[161]

As for defense systems for the private sector, or maintaining cyber-hygiene, many cybersecurity experts believe that basic cyberhygiene is a simple and logical first step in corporate cybersecurity. Estimates suggest that good cyberhygiene could prevent up to eighty-five percent of cyber-intrusions. Rather than waiting for legislative mandates to spur corporate cybersecurity spending, corporations would be wise to consider whether some proactive investments in basic cyber-hygiene are warranted as part of their basic

[159] Id. at, 1707-1708.
[160] Thompson, TEXAS LAW REVIEW, 494 (2011).
[161] Kelly, BOSTON UNIVERSITY LAW REVIEW, 1684-1685 (2012).

corporate responsibility. However, even basic cyberhygiene, let alone sophisticated software such as Einstein, is expensive, if not costprohibitive, for some companies.[162]

If not subsidizing private sector in equipping private sector with cost-prohibitive defense systems, an important source component for developing technical solutions for the private sector can be seen in identification of vulnerabilities, security breaches and potential hazards. This can be achieved by communication crucial findings on vulnerabilities to the network owners and the private sector.[163]

7.2 Standardization and Air-Gapped Networks

Standardization can be seen as both an advantage and a disadvantage. Standards are necessary for the interoperability of products by multiple vendors. Interoperability is critical in communications and national infrastructure, including the national power grid and the medical and financial establishments. The result of the tens of thousands of standards in use toda, is a world that is massively interconnected. The interoperability in critical infrastructural assets helps prevent and hinder cybersecurity risks through, for example, development of improved standards for browser security, application security, and e-mail authentication.[164]

With increased interconnection and unified standards, however, comes increased vulnerability, both to external and internal threats.[165] The use of identical security processes on every computer network does not seem to be an optimal solution – at least not without weighing the competing costs.[166] The negative effect of interoperability is greater potential vulnerability of the entire system, which is easier access to the rest of the systems once a part of it is compromised. This includes spread of viruses and other malware, as well as hacking. The defense for such systems should be absolutely impenetrable to outweigh for the risks, which in itself is a rather remote possibility, if a possibility at all.

---

[162] Teplinsky, AMERICAN UNIVERSITY BUSINESS LAW REVIEW, 313-314 (2013).
[163] Kelly, BOSTON UNIVERSITY LAW REVIEW, 1685-1686 (2012).
[164] Contreras, et al., AMERICAN UNIVERSITY LAW REVIEW, 1117 (2013).
[165] Id. at.
[166] Shane, TEXAS LAW REVIEW, (2012).

Some commentators suggest disconnecting critical system networks from the internet entirely;[167] such systems as power generation and water distribution, core services the nation depends on to remain functioning. The security industry refers to this process as creating an "air gap" between supercritical systems and the general network. Air gaps may be somewhat burdensome, but the security payoff is unparalleled: air-gapped systems are fully isolated and practically impervious unless an attacker manages to physically access the system. [168]

8 Policy Considerations

A viable cybersecurity framework shall aim at the development of the adequate cybersecurity culture. Therefore it shall include national and international cooperative efforts to develop standards, methodologies, procedures, and processes that align policy comprising legislation, business, education and technology approaches to address cyber risks.[169] Given the inclusive and comprehensive nature of the desirable policy framework, the private sector will naturally play as significant a role in the implementation of the policy as does the public sector. At that, the policy on cybersecurity and cybercrime shall be informed by the adequate understanding of the cyber-vulnerability threat on the part of the policy developer.[170]

In this light, perhaps the most critical of all problems connected with the development of a viable cybersecurity policy framework is the problem formulated by Shane as "the current state of public ignorance and indifference to this issue,"[171] which includes executive and legislative authorities of various jurisdictions. Although Shane's analysis concerned the United States, there is, however, no reason to believe that the situation is significantly different in the rest of the world. Although there are many legislative initiatives addressing cybersecurity in many jurisdictions, it is unlikely that executive and legislative authorities of the majority of governments have sufficient understanding of cybersecurity as an actual

[167] RICHARD A. CLARKE & ROBERT KNAKE, CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT 132 (Harper Collins. 2010).
[168] Thompson, TEXAS LAW REVIEW, 494 (2011).
[169] Teplinsky, AMERICAN UNIVERSITY BUSINESS LAW REVIEW, 300 (2013).
[170] Contreras, et al., AMERICAN UNIVERSITY LAW REVIEW, 1117 (2013).
[171] Shane, TEXAS LAW REVIEW, (2012).

problem of policy.[172] That is not to say, of course, that the governments see the matters of cybersecurity as unimportant. Rather, there are no viable and comprehensive policies at place that would aim at cultivation of social awareness of the cyber risks and adequate skills to manage these risks.

The issues of policy suggest considerations that would incentivize the parties with the greatest capacity to improve the security. The public good with regard to public security shall be balanced against other public goods, such as privacy, productivity, economic growth, organizational flexibility, military effectiveness, government transparency, and accountability.[173] To this end, Shane suggests that "only such initiative – which looks at cybersecurity through the eyes of everyone whose interests are implicated – will be adequate to produce the sort of political movement that can produce significant change."[174] At that, policy considerations shall not be based on an "security at all costs" approach and avoid alarmist or sensationalist rhetoric that has no touch with reality, which could lead to weakling of such public goods as government transparency and accountability.[175]

Also, the policy considerations should include longstanding and controversial issues. For example, can the market be relied upon to police itself when it comes to protecting critical infrastructure? What is the government's proper role vis-à-vis the private sector cybersecurity given that the internet is largely private-sector-owned and operated? Would legislative action, such as setting voluntary or obligatory cybersecurity standards for critical infrastructure incentivize the right behavior or inhibit innovation?[176]

To this end, some believe that the most important cybersecurity issue is ensuring that the private sector adequately adheres to standards for critical infrastructure protection and propose that the law enforcement agencies take the lead in creating a regulatory model. Others believe that the most important cybersecurity problem to be solved in the near term

[172] Id. at.
[173] Id. at.
[174] Id. at; See also Kelly, BOSTON UNIVERSITY LAW REVIEW, 1709 (2012).
[175] See e.g. Thompson, TEXAS LAW REVIEW, (2011).
[176] Contreras, et al., AMERICAN UNIVERSITY LAW REVIEW, 1119 (2013).

is ensuring a better flow of information between the private and public sectors and that the intelligence community has the necessary expertise to lead the way.[177]

8.1 Vulnerability Mitigation and Threat Deterrence

Contreras et al suggest that the cybersecurity policy shall be based not only on reactive vulnerability mitigation, that is, on developing protection against cyber-threats, but also, and for the most part, on threat deterrence. Vulnerability mitigation alone cannot provide for the adequate level of sustainable security as even the most sophisticated defenses can be defeated by those with the adequate resources and the will.[178] In this light, the role of the private sector in development of deterrence policies is warranted exactly because the private sector owns a significant portion of critical infrastructure worldwide.

Some countries, such as the United States, which has the largest cyber infrastructure on the planet, has adopted a largely self-regulatory, market-based approach to cybersecurity, relying on the private sector to secure its own networks. In keeping with this approach, no federal agency is responsible for defending the civilian domain, and the federal government has avoided generally-applicable federal mandates regarding private sector cybersecurity practices.[179]

There are two main strategies to address harmful conduct: (i) to react after such conduct has been committed in order to incapacitate and punish the actor(s); (ii) to prevent the conduct from occurring; the two strategies are not necessarily inconsistent. For the last century, there has been an evolving emphasis upon preventing undesirable conduct or crime rather than simply reacting to it occurring. The preventative strategy though still plays a relatively minor role in our overall approach to dealing with real-world crime. One reason why prevention is a small part of the current strategy is that it is resource-intensive; this implies not only qualitative and quantitative increase in policing of the environment in which undesirable conduct may occur, but also collaboration with other cybersecurity participants, such as community members. Of crucial importance in deterrence strategy

[177] Id. at, 1119-1120.
[178] Id. at, 1114.
[179] Teplinsky, AMERICAN UNIVERSITY BUSINESS LAW REVIEW, 232 (2013).

plays creation of a climate in which the commission of crime is seen as a high-risk and therefore unattractive proposition.[180]

The efficacy of the traditional approach to enforcing the criminal law is eroding, at least in part dealing with cybercrime. The traditional model of law enforcement does not seem to be able to deal effectively with cybercrime because online crime possesses few, if any, of the essential characteristics of real-world crime, such as those enumerated above in the introduction.[181] There is therefore the emergence of an alternative approach to law enforcement, one that emphasizes collaboration between the public and private sectors and the prevention of crime rather than merely reacting to it.[182]

The traditional model is a reactive model; its fundamental premise is that officers react to completed crimes by apprehending the perpetrators, who are prosecuted and punished; this renders them incapable of re-offending and ensures that their experience deters others from offending. This is a territorial approach to law enforcement; it assumes that perpetrators, victims and officers are all physically situated in a reasonable degree of proximity within a single territorially-defined state. When these assumptions are valid, the model works; police officers who know the area stand a good chance of being able to identify and apprehend perpetrators, and the local legal system stands a good chance of being able to convict and punish them. However, these assumptions do not hold for cybercrime. The assumptions predicated on territory are irrelevant in dealing with cybercrime.[183]

In addition to the traditional retributive justice, cybercrime deterrence includes the promulgation of legislation, effective leadership, development of criminal justice and law enforcement capacity, education and awareness, the development of a strong knowledge base, and cooperation across government, communities, the private sector and internationally. At that, the cybercrime strategies are likely be closely integrated in

[180] Brenner, RUTGERS COMPUTER AND TECHNOLOGY LAW JOURNAL, 42 (2004).
[181] Id. at, 25.
[182] Id. at, 1-2.
[183] Id. at, 41.

cybersecurity strategies, highlighting components on awareness raising, international cooperation, and law enforcement capacity.[184]

The continued importance of public awareness raising campaigns, including those covering emerging threats, and those targeted at specific audiences, such as children, was highlighted by responding Governments, private sector entities, and academic institutions. User education is most effective when combined with systems that help users to achieve their goals in a secure manner. If user cost is higher than direct user benefit, individuals have little incentive to follow security measures. Private sector entities also report that user and employee awareness must be integrated into a holistic approach to security. Foundational principles and good practice referred to include accountability for acting on awareness, risk management policies and practices, board-level leadership, and staff training. Two-thirds of private sector respondents had conducted a cybercrime risk assessment, and most reported use of cybersecurity technology such as firewalls, digital evidence preservation, content identification, intrusion detection, and system supervision and monitoring. Concern was expressed, however, that small and medium-sized companies either do not take sufficient steps to protect systems, or incorrectly perceive that they will not be a target.[185]

Regulatory frameworks have an important role to play in cybercrime prevention, both with respect to the private sector in general and service providers in particular. Nearly half of countries have passed data protection laws, which specify requirements for the protection and use of personal data. Some of these regimes include specific requirements for internet service providers and other electronic communications providers. While data protection laws require personal data to be deleted when no longer required, some countries have made exceptions for the purposes of criminal investigations, requiring internet service providers to store specific types of data for a period of time. Many developed countries also have rules requiring organizations to notify individuals and regulators of data breaches. Internet service providers typically have limited liability as mere conduits of data. Modification of transmitted content increases liability, as does actual or constructive knowledge of an illegal activity. Expeditious action after notification, on the other hand,

[184] Comprehensive Study on Cybercrime xxvi. 2013.
[185] Id. at, xxvi-xxvii.

reduces liability. While technical possibilities exist for filtering of internet content by service providers, restrictions on internet access are subject to foreseeability and proportionality requirements under international human rights law protecting rights to seek, receive and impart information.[186]

Public-private partnerships are central to cybercrime prevention. Over half of all countries report the existence of partnerships. These are created in equal numbers by informal agreement and by legal basis. Private sector entities are most often involved in partnerships, followed by academic institutions, and international and regional organizations. Partnerships are mostly used for facilitating the exchange of information on threats and trends, but also for prevention activities, and action in specific cases. Within the context of some public-private partnerships, private sector entities have taken proactive approaches to investigating and taking legal action against cybercrime operations. 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 through delivery of education and training to professionals, law and policy development, and work on technical standards and solution development. Universities house and facilitate cybercrime experts, some computer emergency response teams (CERTs), and specialized research centres.[187]

Crime prevention draws upon the criminologies of everyday life to focus upon the reduction of opportunity by increasing the level of effort needed to commit a crime, increasing the risks to the offender, or reducing the reward of crime. Crucial to the success of crime control policies is the ability of the implementer not only to control the design process of the technology and its support systems, but also to be able to identify and vulnerabilities and then to be able to modify design accordingly prior to production.[188]

8.2 Private-Public Sector Dynamic

As mentioned above, the role of the private sector in policy consideration can be structured two-fold – (i) cooperation between the private and public sectors and (ii) introduction by

[186] Id. at, xxvii.
[187] Id. at.
[188] WALL, Cybercrime: The Transformation of Crime in the Information Age 187-188. 2007.

the public sector of cybersecurity standards and their enforcement through imposition of administrative and/or criminal sanctions, as well as creating cybersecurity infrastructure in the form of specialized regulatory agencies. These two dimensions of the dynamic between the private and the public sectors are not mutually exclusive.

The basic problem of cooperation between the public and private sectors is the lack of incentives sufficient to make companies in most critical infrastructure sectors take voluntary action to bring the security of their networks to the level needed for national security.[189] The main theme tension between the public and private sectors is seeking forms of justice that represent their different interests.[190] The relatively low levels of prosecutions for breaches of computer security and low levels of recorded internet-related fraud are poignant examples of this tension. They suggest that most breaches of security tend to be dealt with by victims rather than the police, highlighting the preference of the private sector to seek private justice solutions instead of invoking the public criminal justice process that might expose their weaknesses to customers or commercial competitors. This indicates that the model of criminal justice offered to corporate victims by the police and other public law enforcement agencies is not generally regarded as conductive to their business interest.[191]

A key challenge to achieving an adequate private sector investment in cybersecurity is the fact that cybersecurity is a public good. One company's underinvestment in cybersecurity can redound to the detriment of other companies with whom they connect. While some companies may be motivated to invest sufficiently to protect their own assets, others are unlikely to invest sufficiently to protect the assets of companies with whom they do business, leading some experts to conclude that the private sector is unlikely to supply adequate cybersecurity on its own.[192]

[189] Teplinsky, AMERICAN UNIVERSITY BUSINESS LAW REVIEW, 305 (2013).
[190] Id. at, 306-307.
[191] WALL, Cybercrime: The Transformation of Crime in the Information Age 25-26. 2007; MEHAN, Cyberwar, Cyberterror, Cybercrime: A Guide to the Role of Standards in an Environment of Change and Danger 78-81. 2008.
[192] Teplinsky, AMERICAN UNIVERSITY BUSINESS LAW REVIEW, 310 (2013).

The dilemma of the private-public sector dynamic can be illustrated with the following example. In the United States, the so called Task Force Proposal[193] reveals a hesitation to endorse any legislative package that contains a significant level of federal government involvement in cybersecurity. This hesitation is primarily motivated by two beliefs: (i) the need for fiscal savings, and (ii) the superiority of market incentives over direct regulation for private entities. This approach contrasts sharply with the so called Obama Proposal, the Cybersecurity Legislative Proposal, which envisions considerable investment in cybersecurity infrastructure coupled with directly mandated cybersecurity standards for the private market. Second, the Task Force Proposal would create a non-governmental agency to establish cybersecurity standards for private entities, where the Obama Proposal would delegate that authority to the federal law enforcement agencies, such as the Department of Homeland Security. Moreover, while the Task Force Proposal standards would be voluntary, the standards promulgated by the law enforcement agencies under the Obama Proposal would be mandatory for covered entities.[194]

This dynamic underlies a fundamental problem of the situation with legal regulation of cybersecurity and cybercrime in that law, policy, and market mechanisms are experiencing significant difficulty keeping pace with the rapid and enormous technological changes. Although industry has made significant changes to address cybercrime, there is a dire need

[193] At least twenty-two different cybersecurity-related legislative proposals, in the form of Congressional bills, executive proposals, and formal recommendations from a Republican House of Representatives task force. For detail see: Identifying Cybersecurity Risks to Critical Infrastructure Act of 2012, H.R. 6221, 112th Cong. (2012); Cybersecurity Act of 2012, S. 3414, 112th Cong. (2012); Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology (SECURE IT) Act of 2012, S. 3342, 112th Cong. (2012); Federal Information Security Amendments Act of 2012, H.R. 4257, 112th Cong. (2012); Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology (SECURE IT) Act of 2012, S. 2151, 112th Cong. (2012); Cybersecurity Act of 2012, S. 2105, 112th Cong. (2012); Promoting and Enhancing Cybersecurity and Information Sharing Effectiveness (PRECISE) Act of 2011, H.R. 3674, 112th Cong. (2011); Cyber Intelligence Sharing and Protection Act, H.R. 3523, 112th Cong. (2012); Personal Data Protection and Breach Accountability Act of 2011, S. 1535, 112th Cong. (2011); International Cybercrime Reporting and Cooperation Act, S. 1469, 112th Cong. (2011); Data Security Act of 2011, S. 1434, 112th Cong. (2011); Data Breach Notification Act of 2011, S. 1408, 112th Cong. (2011); Secure and Fortify Electronic (SAFE) Data Act, H.R. 2577, 112th Cong. (2011); Cybersecurity Enhancement Act of 2011, S. 1152, 112th Cong. (2011); Personal Data Privacy and Security Act of 2011, S. 1151, 112th Cong. (2011); Cybersecurity Enhancement Act of 2012, H.R. 2096, 112th Cong. (2012); Cybersecurity and Internet Freedom Act of 2011, S. 413, 112th Cong. (2011); Cybersecurity and Internet Safety Standards Act, S. 372, 112th Cong. (2011); Cyber Security and American Cyber Competitiveness Act of 2011, S. 21, 112th Cong. (2011); Homeland Security Cyber and Physical Infrastructure Protection Act of 2011, H.R. 174, 112th Cong. (2011).

[194] Kelly, BOSTON UNIVERSITY LAW REVIEW, 1696-1697 (2012).

to find policies that will incent the right behaviors without dampening the innovation needed for both good security and a robust economy.[195]

9 International Cooperation in Criminal Matters

The natural independent character of the network and information infrastructure and its growing importance for economies, public safety and our society in general makes controlling and countering potential threats a demanding and critical challenge for both governments and enterprises.[196] Many cybercrime acts involve a transnational dimension, engaging issues of transnational investigations, sovereignty, jurisdiction, extraterritorial evidence, and a requirement for international cooperation.[197] The issues of cooperation are of utmost importance for any effective regulation of globalized networked technologies. International best practice, if not international cooperation and collaboration, is more evident in the area of cybercrime, perhaps due in part to the near universality of the substantive provisions of the Budapest Convention.[198]

It often is said that cybercrime knows no borders, meaning that criminals can with ease and effectiveness commit crimes across national boundaries through the use of the internet and associated electronic communications. This observation is then contrasted with the traditional limitations faced by law enforcement agencies and judicial systems, which remain stubbornly circumscribed by geographical limitations on investigative, prosecution, and judicial powers, as in the observation, cybercrime knows no borders, yet the criminal law remains fundamentally territorial in nature.[199]

Despite the fact that many attacks are carried out across multiple jurisdictions and often originate in foreign countries, current international law does not recognize nations as duty bound to assist in investigating a cyberattack that allegedly originated within their jurisdiction. As a result, nations attempting to develop and enforce cybersecurity measures often lack international support from nations where a given cyberattack likely originated.

---

[195] Contreras, et al., AMERICAN UNIVERSITY LAW REVIEW, 1120 (2013).
[196] Kremer & Müller, Cyberspace and International Relations: Theory, Prospects and Challenges 42-44. 2014.
[197] Comprehensive Study on Cybercrime xxiv-xxv. 2013.
[198] Satola & Judy, WILLIAM MITCHELL LAW REVIEW, 1771 (2011).
[199] Urbas, JOURNAL OF INTERNET LAW, 1 (2012).

Even when a victimized nation does receive cooperation from a foreign nation under, for example, a Mutual Legal Assistance Treaty (MLAT), evidentiary requests often take several months to be honored, if at all. Since evidence of a cyberattack may be disposed of quickly, current international agreements like MLATs providing for law enforcement cooperation operate too slowly to be effective.[200]

No nation-state can achieve adequate cybersecurity on its own; international coordination and cooperation must be part of the response.[201] The current international cooperation takes no account of the specificities of electronic evidence and the global nature of cybercrime. This is particularly the case for cooperation in investigative actions. A lack of common approach, including within current multilateral cybercrime instruments, means that requests for actions, such as expedited preservation of data outside of those countries with international obligations to ensure such a facility and to make it available upon request, may not be easily fulfilled. Globally, divergences in the scope of cooperation provisions in multilateral and bilateral instruments, a lack of response time obligation, a lack of agreement on permissible direct access to extraterritorial data, multiple informal law enforcement networks, and variance in cooperation safeguards, represent significant challenges to effective international cooperation regarding electronic evidence in criminal matters.[202]

Moreover, sovereignty and other issues present countries with inherently conflicting policy objectives and cultural clashes, including the need to balance different interests and rights such as security and privacy, and are compounded by the impact of rapidly developing technologies on the structure of any agreement.[203]

Despite the challenges, in recent years there have been notable law enforcement successes. Some of these have involved a high degree of international law enforcement cooperation, assisted by modernized understandings of legal jurisdiction and the use of cross-border mechanisms such as mutual legal assistance and extradition.[204] Because law enforcement

[200] Stahl, GEORGIA JOURNAL OF INTERNATIONAL AND COMPARATIVE LAW, 249-250 (2011).
[201] Satola & Judy, WILLIAM MITCHELL LAW REVIEW, 1783 (2011).
[202] Comprehensive Study on Cybercrime xxvi. 2013.
[203] Satola & Judy, WILLIAM MITCHELL LAW REVIEW, 1772 (2011).
[204] Urbas, JOURNAL OF INTERNET LAW, 1-8 (2012).

powers generally do not extend beyond national boundaries, for example, allowing police from one country to travel to and investigate crimes in others without the permission of the latter, cross-border investigations usually depend on cooperation at national agency or even local officer level. Cooperation can occur with minimal formality, through temporary officer-to-officer contacts, or through more established channels of communication such as 24/7 contact points for law enforcement, as envisaged in the Council of Europe's Convention on Cybercrime.[205]

Forms of international cooperation include extradition, mutual legal assistance, mutual recognition of foreign judgments, and informal police-to-police cooperation.[206] Due to the volatile nature of electronic evidence, international cooperation in criminal matters in the area of cybercrime requires timely responses and the ability to request specialized investigative actions, such as preservation of computer data. Response times for formal mechanisms, that are used currently, are of the order of months, for both extradition and mutual legal assistance requests, a timescale which presents challenges to the collection of volatile electronic evidence.[207] Initiatives and innovations for informal cooperation and for facilitation of formal cooperation, such as 24/7 networks, offer important potential for faster response times.[208]

Formal and informal modes of cooperation are designed to manage the process of State consent for the conduct of foreign law enforcement investigations that affect a state's sovereignty. Increasingly, however, investigators, knowingly or unknowingly, access extraterritorial data during evidence gathering, without the consent of the state where the data is physically situated. This situation arises, in particular, due to cloud computing technologies which involve data storage at multiple data centres in different geographic locations. Data 'location', whilst technically knowable, is becoming increasingly artificial, to the extent that even traditional mutual legal assistance requests will often be addressed to the country that is the seat of the service provider, rather than the country where the data centre is physically located. Direct foreign law enforcement access to extraterritorial data

[205] Id. at, 9.
[206] BRENNER, Cybercrime and the Law: Challenges, Issues, and Outcomes 178-179. 2012.
[207] Comprehensive Study on Cybercrime xxv. 2013; BRENNER, Cybercrime and the Law: Challenges, Issues, and Outcomes 179-182. 2012.
[208] Comprehensive Study on Cybercrime xxv. 2013.

could occur when investigators make use of an existing live connection from a suspect's device, or where investigators use lawfully obtained data access credentials. Law enforcement investigators may, on occasion, obtain data from extra-territorial service providers through an informal direct request, although service providers usually require due legal process.[209]

Examples of such cooperation between law enforcement officers in different countries are provided by several recent cases in which Australian suspects have been prosecuted in relation to child grooming. In one case, Australian Federal Police (AFP) were alerted by their New Zealand counterparts that a Canberra man had been communicating sexually online with a supposedly 14 year-old girl named 'Roxanne,' in reality a fictional identity used by an Auckland police officer to track online child groomers. AFP officers arranged a meeting in Canberra between the 'girl' and the suspect, at which he was arrested and then charged. In another case, AFP officers were first alerted by German police that a Canberra resident had been downloading material from a child pornography Web site, and later by the FBI that he had been in contact with a supposedly 14 year-old boy named 'Brad' in the state of New Hampshire, actually a fictitious identity used by an FBI agent. In subsequent correspondence, the FBI agent and his AFP counterpart agreed to have "Brad" introduce the suspect online to 'Jamie,' a 12 year-old boy in Canberra, who was actually an AFP investigator. At an arranged meeting with "Jamie" the suspect was arrested and then charged.[210]

Such examples depend on relationships of trust that have been developed through regular contact between law enforcement agencies or officers in different countries. Among countries such as Australia, New Zealand, Canada, the United States, and many European states, sufficient contacts have been made over many years to facilitate highly effective cooperation. With states in Eastern Europe or in developing countries, new relationships have been forged. For example, in the last decade or so, the US Department of Justice (DOJ), particularly through its Computer Crime and Intellectual Property Section (CCIPS), has successfully fostered cooperative relationships with law enforcement agencies in Belarus,

[209] Id. at, xxv-xxvi.
[210] Urbas, JOURNAL OF INTERNET LAW, 9 (2012).

Bulgaria, Estonia, Poland, Romania, and the Ukraine as well as its more traditional partners to disrupt international cybercrime groups and bring their members to justice.[211]

In the most sophisticated of such co-operative arrangements, law enforcement agencies in several countries are able to share operational information and co-ordinate critical actions in real time so that search warrant executions and arrests occur simultaneously in different locations across the globe. Clearly, this is important in ensuring that all members of globally dispersed groups can be apprehended before they have an opportunity to flee or to destroy evidence. Significant internationally coordinated enforcement actions have been reported against international child exploitation rings and global copyright piracy groups.[212]

An example is the recent Operation Delego, which resulted in the dismantling of an online pedophile network using a private, highly encrypted bulletin board known as Dreamboard. This network included more than 500 members, and its strict rules of access and membership, which required the posting of child exploitation material including images of children who were abused specifically to produce new material for the network, were printed in English, Russian, Japanese, and Spanish. The international enforcement operation resulted in the charging of 72 members with conspiring to advertise and distribute child pornography and 50 also were charged with engaging in a child pornography enterprise, located across five continents and 13 countries: Canada, Denmark, Ecuador, France, Germany, Hungary, Kenya, the Netherlands, the Philippines, Qatar, Serbia, Sweden, and Switzerland. This involved the collaborative efforts of the DOJ and Immigration and Customs Enforcement (ICE), the European Union's Judicial Cooperation Unit, and the law enforcement agencies of the other countries involved.[213]

The private, governmental, and non-governmental sectors, on the basis of both national and international efforts, have been taking steps to increase the security of their products, services, and networks. These efforts include, for example, the work of international standards bodies, which range from the treaty-based International Telecommunication

[211] Id. at.
[212] Id. at.
[213] Id. at, 9-10.

Union (ITU) to non-governmental but highly influential and essential bodies such as the Internet Engineering Task Force (IETF). Important issues for consideration include the role of standards and the role of government in developing standards.[214]

Despite the positive examples of cooperation, in terms of an evolving cybersecurity legal framework, there are a number of evident vulnerabilities and impediments to effective international cooperation. Among these are:[215]

Dissonance in national approaches to cybersecurity. Different countries, even members of the same regional organizations, can take different approaches to the concept of cybersecurity in terms of national policies, laws, and implementation. Some countries see Internet governance as having state security at its core, by which they mean that the State can know exactly who sent and received every transmission, every transmission's traceroute, and the contents of every transmission; it can delete, block, and/or seize any transmission of which it disapproves; and it can punish efficiently those who send or receive unapproved transmissions. At the other end of the spectrum are countries and organizations that strongly believe that proper Internet governance, including Internet security, must be integrated and balanced with the type of freedoms protected by instruments such as the First, Fourth, Fifth, and Fourteenth Amendments of the United States Constitution, the European Union Charter of Fundamental Rights, and numerous United Nations human rights documents. This "dissonance" can lead to a lack of effective coordination and can result in part because of a lack of multi-stakeholder participation in both policy-making and legislation.[216]

Cybersecurity is a twenty-first century problem that requires twenty-first century responses. However, in the legal sphere, many concepts developed in an analog era simply do not apply in a digital era or they cause friction when applied. For example, the lack of consensus on the fundamental and related issues of jurisdiction and sovereignty make it difficult to effectively cross borders to address international cybersecurity incidents. A nation state may view its sovereignty as being impaired if another nation state may

[214] Satola & Judy, WILLIAM MITCHELL LAW REVIEW, 1755 (2011).
[215] Id. at, 1749.
[216] Id. at, 1750.

exercise 'jurisdiction' within its borders. However, nation states may view their sovereignty as being enhanced if by mutual agreement they obtain jurisdiction within each other's territories. In order for the rule of law to prevail, the inherent cross-border nature of cyberspace seems to require such agreements for the mutual expansion of jurisdiction.[217]

Existing tools and instruments are not fully applied or are only partially implemented. Another source of vulnerabilities in the existing cybersecurity legal frameworks results from failure to apply the terms of existing instruments or only partial implementation of such instruments. Legal systems are increasingly responding to this source of vulnerability by establishing liability for failure to implement existing cybersecurity tools in a manner proportional to the sensitivity of the data held. This liability may be imposed because proportional security mechanisms were not employed as promised or regardless of whether a promise was made. However, this liability is often imposed on a case-by-case basis and not pursuant to statutory or regulatory requirements aimed at the particular issue.[218]

10 Treaty-Based Approach to Cybersecurity and Cybercrime

The international community has a clear interest in developing a comprehensive, multilateral cybersecurity framework because the widespread use of the internet in every aspect of daily life has created an almost irreversible dependence on its technological benefits, and because the conceptual underpinnings of existing legal frameworks are not readily adaptable to threats emerging in cyberspace.[219]

No comprehensive international legal framework addressing cybersecurity exists. International efforts to address the issue have been narrow in scope, focusing primarily on data privacy regulations and human rights, at the expense of a broader effort to define and differentiate various levels of cyberaggression and codify an international approach to deal

[217] Id. at, 1750-1751.
[218] Id. at, 1751.
[219] Stahl, GEORGIA JOURNAL OF INTERNATIONAL AND COMPARATIVE LAW, 249 (2011).

with its challenges.[220] In the absence of codified law, nations attempting to enforce their cybersecurity regimes against foreign perpetrators have done so largely by analogy to international law governing military use of force[221] and domestic criminal law. Existing international cybersecurity agreements are narrow in scope, focusing on criminal activity in cyberspace, and fail to adequately account for cyberspace as a platform for terrorism and military action.[222]

These shortcomings may be due, in part, to the nature of cyberaggression, which challenges the conceptual categories we have so far used to avoid chaos and maintain order in our societies and in our lives. Without a comprehensive international definition of the types of cyberaggression, nations will continue to face challenges in assessing the legality of their response to a given attack. Also, because there is no international body authorized to investigate and prosecute cyberaggression without limitation based upon the attack's location, nations resort to legal systems founded on the principle of territorial jurisdiction in crafting a response to cyberattacks. Nations' efforts are hampered by the fact that international law recognizes no duty to assist other nations in investigating cyberaggression absent an explicit agreement to the contrary among the parties.[223]

A comprehensive international treaty is wanting on some or all aspects of the cybersecurity problem.[224] When analyzing the merits of a treaty-based approach to cybersecurity, a myriad of questions arise, including: What are the key issues that should or could be addressed in a cybersecurity treaty? What would be the added value of such a treaty? What would be the risks? What prior efforts have been attempted and what caused them to fail or have limited effect? What incremental steps can be taken to break through the problems? How can treaty compliance be verified? How could countries globally be supported in the strengthening of their cybersecurity capacities, through technical assistance and other means?[225]

---

[220] Id. at, 260-261.
[221] See e.g. Schmitt, Tallinn Manual on the International Law Applicable to Cyber Warfare. 2013.
[222] Stahl, GEORGIA JOURNAL OF INTERNATIONAL AND COMPARATIVE LAW, 250 (2011).
[223] Id. at, 260-261.
[224] Satola & Judy, WILLIAM MITCHELL LAW REVIEW, 1783-1784 (2011).
[225] Id. at, 1785.

Any effort to reach international consensus on cybersecurity is likely to expose a range of concerns, which in part flow from different visions of national security, of the role and value of the internet, of human rights, and of economic policy. Some see cybersecurity as having state security at its core, which leads to an emphasis on capabilities to monitor and attribute transmissions and to block any undesirable content. Others strongly believe that internet governance (including internet security) involves the integrating and balancing of interests, including not only national security, but also human rights and the economic and developmental interests associated with a vibrant, innovative, and competitive ICT sector. These differing perspectives manifest themselves in many areas, including, for example, the increasing debate over the issue of attribution, referred to above.[226]

Although no significant developments in the promulgation of a cybersecurity treaty have been seen in the last decade, the promulgation of international and regional instruments aimed at countering cybercrime have been more successful. These include binding and nonbinding instruments. Five clusters of international or regional instruments can be identified, consisting of instruments developed in the context of, or inspired by: (i) the Council of Europe or the European Union, (ii) the Commonwealth of Independent States or the Shanghai Cooperation Organization, (iii) intergovernmental African organizations, (iv) the League of Arab States, and (v) the United Nations.[227]

These clusters are not absolute and a significant amount of crossfertilisation exists between the instruments. The basic concepts developed in the Council of Europe Cybercrime Convention, for example, are also found in many other instruments. United Nations entities, such as UNECA and ITU, have also had some involvement in the development of instruments in the African context, including the Draft African Union Convention.[228]

A number of the instruments – notably the Council of Europe Conventions, the European Union instruments, the Commonwealth of Independent States Agreement, the Shanghai Cooperation Organization Agreement, and the League of Arab States Convention – are

[226] Id. at, 1785-1786.
[227] Comprehensive Study on Cybercrime 63. 2013.
[228] Id. at, 64.

express agreements between states intended to create legal obligations. Many of these treaties are non-binding. Instruments – such as the Commonwealth Model Law, the COMESA Draft Model Bill, the League of Arab States Model Law, and the ITU/CARICOM/CTU Model Legislative Texts – are not intended to create legal obligations for states. Rather, they are designed to serve as inspiration or 'models' for development of national legislative provisions. Non-binding instruments may nonetheless have a significant influence at the global or regional level when many states choose to align their national laws with model approaches.[229]

The Council of Europe Cybercrime Convention has the largest number of signatures or ratifications/accessions (48 countries), including five Non-member States of the Council of Europe (Argentina, Chile, Costa Rica, Dominican Republic, Mexico, Panama, Philippines, and Senegal). Other instruments have smaller geographic scope – the League of Arab States Convention (18 countries or territories), the Commonwealth of Independent States Agreement (10 countries), and the Shanghai Cooperation Organization Agreement (6 countries). If signed or ratified by all member states of the African Union, the Draft African Union Convention could have up to 54 countries or territories.[230] The AU Convention will also be binging for states.

The enumerated international instruments exhibit differences in substantive focus. Many of these differences derive from the underlying aim of the instrument. Some instruments, such as the Council of Europe Cybercrime Convention, the Commonwealth Model Law, the League of Arab States Convention, and the Commonwealth of Independent States Agreement, aim specifically to provide a criminal justice framework for combating forms of cybercrime. Others, such as the Shanghai Cooperation Organization Agreement and the Draft African Union Convention, take a broader approach, of which cybercrime is just one component. The Shanghai Cooperation Organization Agreement, for example, addresses cooperation in cybercrime matters within the context of international information security – including information warfare, terrorism and threats to global and national information infrastructures. The Draft African Union Convention takes a cybersecurity-based approach that includes organization of electronic transactions, protection of personal data,

[229] Id. at, 65.
[230] Id. at, 67-68.

promotion of cybersecurity, e-governance and combating cybercrime. Such differences significantly affect the way in which cybercrime is 'framed' within the international or regional legal response. Due to its broader focus on international information security, for example, the Shanghai Cooperation Organization Agreement does not set out specific cyber acts that should be criminalized. Similarly – perhaps due to its focus on cybersecurity as a whole, rather than criminal justice in particular – the Draft African Union Convention presently does not seek to establish mechanisms of international cooperation in cybercrime criminal matters.[231]

11 General Recommendations

There are two major areas that are in need of governmental attention at the moment: (i) development of comprehensive and clear policies on cybersecurity, and (ii) development and adoption of relevant legislation supporting the policy that would enhance cybersecurity.

The considerations of the policy is of utmost importance and should include first and foremost long-term educational efforts on all levels of society including general education on cybersecurity matters, as well as professional education of law enforcement, judiciary and legislative authorities. Also, an important component of a viable policy is promoting international discussion on the issues cybersecurity and its management on an international level.

While international cooperation is necessary, each nation will have to develop, as a foundation, its own national cybersecurity strategy, authorities, and capabilities. Within any given nation state, adequate cybersecurity will require effective coordination and cooperation among governmental entities on the national and sub-national levels as well as the private sector and civil society.

From the crime prevention and criminal justice perspective, six key areas may benefit from either binding or non-binding guidance at international or regional level: (i) criminalization; (ii) law enforcement procedural powers; (iii) procedures regarding

[231] Id. at, 69.

electronic evidence; (iv) state jurisdiction in cybercrime criminal matters; (v) international cooperation in cybercrime criminal matters; and (vi) the responsibility of service providers.

Issues for consideration in the area of private sector involvement include: What are the most effective means to promote effective coordination and cooperation at the national level? To what extent should cooperation of the private sector be legally compelled? What incentives or subsidies may promote cooperation? How far should governments go in regulating the private sector in the name of improving cybersecurity? What is the role of civil liability systems in addressing cyber-vulnerabilities? As governments seek to develop their own national policies and structures for cybersecurity, questions include: Which agency or ministry should have the lead? What should be the role of civilian agencies versus national security agencies? What should be the roles of law enforcement or national security agencies versus the roles of ministries for trade, commerce, or communications?

12 Bibliography and Consulted Literature

Convention on Cybercrime. Council of Europe. (2001).

Comprehensive Study on Cybercrime (John Sandage, et al. eds., United Nations Office on Drugs and Crime 2013).

Susan W. Brenner, *The Privacy Privilege: Law Enforcement, Technology and the Constitution*, 7 JOURNAL OF TECHNOLOGY LAW & POLICY (2002).

Susan W. Brenner, *Toward a Criminal Law for Cyberspace: a New Model of Law Enforcement?*, 30 RUTGERS COMPUTER AND TECHNOLOGY LAW JOURNAL (2004).

Susan W. Brenner, *Toward a Criminal Law for Cyberspace: Distributed Security*, 10 BOSTON UNIVERSITY JOURNAL OF SCIENCE & TECHNOLOGY LAW (2004).

Susan W. Brenner, *Toward a Criminal Law for Cyberspace: Product Liability and Other Issues*, 5 UNIVERSITY OF PITTSBURGH JOURNAL OF TECHNOLOGY LAW AND POLICY (2005).

SUSAN W. BRENNER, CYBERCRIME AND THE LAW: CHALLENGES, ISSUES, AND OUTCOMES (Northeastern University Press. 2012).

Susan W. Brenner & Bert-Jaap Koops, *Approaches to Cybercrime Jurisdiction*, 4 JOURNAL OF HIGH TECHNOLOGY LAW (2004).

Susan W. Brenner & Joseph Schwerha, *Transnational Evidence-Gathering and Local Prosecution of International Cybercrime*, 20 JOHN MARSHALL JOURNAL OF COMPUTER AND INFORMATION LAW (2002).

Francesco Calderoni, *The European Legal Framework on Cybercrime: Striving for an Effective Implementation*, 54 CRIME, LAW AND SOCIAL CHANGE (2010).

RICHARD A. CLARKE & ROBERT KNAKE, CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT (Harper Collins. 2010).

JONATHAN CLOUGH, PRINCIPLES OF CYBERCRIME (Cambridge University Press. 2010).

Jorge L. Contreras, et al., *Mapping Today's Ceybersecurity Landscape*, 62 AMERICAN UNIVERSITY LAW REVIEW (2013).

Mark F. Grady & Francesco Parisi, The Law and Economics of Cybersecurity (Cambridge University Press 2006).

Craig B. Greathouse, *Cyber War and Strategic Thought: Do the Classic Theorists Still Matter?*, *in* CYBERSPACE AND INTERNATIONAL RELATIONS: THEORY, PROSPECTS AND CHALLENGES (Jan-Frederik Kremer & Benedikt Müller eds., 2014).

THOMAS J. HOLT, CYBERCRIME AND CRIMINOLOGICAL THEORY: FUNDAMENTAL READINGS ON HACKING, PIRACY, THEFT, AND HARASSMENT (Cognella. 2013).

Yvonne Jewkes & Majid Yar, Handbook of Internet Crime (Routledge 2010).

MARK JOHNSON, CYBER CRIME, SECURITY AND DIGITAL INTELLIGENCE (Gower. 2013).

Brian B. Kelly, *Investing In a Centralized Cybersecurity Infrastructure: Why "Hacktivism" Can And Should Influence Cybersecurity Reform* 92 BOSTON UNIVERSITY LAW REVIEW (2012).

Sascha Knoepfel, *Clarifying the International Debate on Stuxnet: Arguments for Stuxnet as an Act of War in* CYBERSPACE AND INTERNATIONAL RELATIONS: THEORY, PROSPECTS AND CHALLENGES (Jan-Frederik Kremer & Benedikt Müller eds., 2014).

Jan-Frederik Kremer & Benedikt Müller, Cyberspace and International Relations: Theory, Prospects and Challenges (Springer 2014).

NIR KSHETRI, CYBERCRIME AND CYBERSECURITY IN THE GLOBAL SOUTH (Palgrave Macmillan. 2013).

Howard F. Lipson, Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues (Software Engineering Institute 2002).

JULIE E. MEHAN, CYBERWAR, CYBERTERROR, CYBERCRIME: A GUIDE TO THE ROLE OF STANDARDS IN AN ENVIRONMENT OF CHANGE AND DANGER (IT Governance Publishing. 2008).

ROBERT MOORE, CYBERCRIME: INVESTIGATING HIGH-TECHNOLOGY COMPUTER CRIME (Anderson Publishing 2011).

Brian Nichiporuk & Carl H. Builder, *Societal Implications*, *in* IN ATHENA'S CAMP: PREPARING FOR CONFLICT IN THE INFORMATION AGE (John Arquilla & David Ronfeldt eds., 1997).

Ellen S. Podgor, *International Computer Fraud: A Paradigm for Limiting National Jurisdiction*, 35 U.C. DAVIS LAW REVIEW (2002).

David Satola & Henry L. Judy, *Towards a Dynamic Approach to Enhancing International Cooperation and Collaboration in Cybersecurity Legal Frameworks: Reflections on the Proceedings of the Workshop on Cybersecurity Legal Issues at the 2010 United Nations Internet Governance Forum* 37 WILLIAM MITCHELL LAW REVIEW (2011).

Michael N. Schmitt, Tallinn Manual on the International Law Applicable to Cyber Warfare (Cambridge University Press 2013).

Peter M. Shane, *Cybersecurity: Toward a Meaningful Policy Framework*, 90 TEXAS LAW REVIEW (2012).

Mathhew J. Sklerov, *Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect Their Duty to Prevent*, 201 MILITARY LAW REVIEW (2009).

William M. Stahl, *The Uncharted Waters of Cyberspace: Applying the Principles of International Maritime Law to the Problem of Cybersecurity*, 40 GEORGIA JOURNAL OF INTERNATIONAL AND COMPARATIVE LAW (2011).

Melanie Teplinsky, *Fiddling on the Roof: Recent Developments in Cybersecurity*, 2 AMERICAN UNIVERSITY BUSINESS LAW REVIEW (2013).

Karson K. Thompson, *Not Like an Egyptian: Cybersecurity and the Internet Kill Switch Debate*, 90 TEXAS LAW REVIEW (2011).

Gregor Urbas, *Cybercrime, Jurisdiction and Extradition: The Extended Reach of Cross-Border Law Enforcement*, 16 JOURNAL OF INTERNET LAW (2012).

DAVID S. WALL, CYBERCRIME: THE TRANSFORMATION OF CRIME IN THE INFORMATION AGE (Polity Press. 2007).

Alamie M. Weber, *The Council of Europe's Convention on Cybercrime*, 18 BERKELEY TECHNOLOGY LAW JOURNAL (2014).

MAJID YAR, CYBERCRIME AND SOCIETY (SAGE. 2006).