DE GRUYTER DOI 10.1515/jhsem-2012-0007 — Homeland Security & Emergency Management 2013; 10(1): 1–27

Angelyn Flowers, Sherali Zeadally* and Acklyn Murray

Cybersecurity and US Legislative Efforts to address Cybercrime

Abstract: Deficiencies in cybersecurity may be the greatest national security threat facing the US in the 21st century. Public and private sector organizations as well as individuals are vulnerable, and the nation's critical infrastructures are also put at risk by these deficiencies. Security professionals, designers, and engineers are currently faced with the challenge of securing cyberspace. Essential to this effort is the necessity to ensure that the nation's laws are adequate to protect against, prevent, and deter cyberattacks. In this article we present a comprehensive review of current US laws and regulations that are being used to deter cybercrime activities and support cybersecurity. We describe legislation presented in the 112th Congress aimed at strengthening laws in fighting cybercrimes and ensuring a high level of cybersecurity, and we briefly review legislative efforts being undertaken in other countries. Finally, we discuss some future issues to be addressed in the growing area of cyberlaw.

Keywords: cybersecurity; cyberattack; cybercrime; law.

***Corresponding author: Sherali Zeadally,** Department of Computer Science and Information Technology, University of the District of Columbia, Washington DC, USA, e-mail: szeadally@udc.edu
Angelyn Flowers: Department of Criminal Justice, University of the District of Columbia, Washington DC, USA
Acklyn Murray: Department of Computer Science and Information Technology, University of the District of Columbia, Washington DC, USA

1 Introduction

When this article was initially written, it began with a prediction that by the time of publication. It is not inconceivable that by the time this article is published, President Obama may have issued an Executive Order on Cybersecurity necessitated in large part by Congressional failure to act. That Executive Order, entitled "Improving Critical Infrastructure Cybersecurity, was issued on February 12, 2013 with the intent to enhance cybersecurity through a voluntary information sharing program between government agencies and private sector critical infrastructure

owners and operators. It also calls for the development of a Cybersecurity Framework to assist critical infrastructure owners and operators in the identification, assessment and management of cyber risk.[1] This is consistent with the President's identification of cybersecurity as one of the nation's most serious economic and national security challenges, and his warnings that the nation's economic prosperity in the 21st century depends on the extent to which we can secure cyberspace.[2] Yet the legacy of the 112th Congress with regard to cybersecurity legislation has been one of intense activity in terms of the variety of legislation introduced, but of very little action in terms of legislation actually passed. Within a month of the defeat of the Cybersecurity Act of 2012 in August, the White House began circulating a draft executive order that would impose voluntary critical infrastructure standards on companies electing to meet cybersecurity best practices and standards.[3] Critical infrastructure includes agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemical industry, postal, and shipping.[4] Senate Majority Leader Harry Reid's failure to bring the Cybersecurity Act of 2012 back for a second vote in the lame duck session of the 112th Congress increased the expectation of a presidential executive order.[5] This expectation bore fruit at the beginning of President Obama's second term; however, the Executive Order is limited and lacks the expansive nature that Congressional legislation can provide. This, therefore, represents a crucial point in time to take stock of the current state of the nation's cyber protection – both what exists and what is needed.

It is unfortunate that the need for legislative change often does not become apparent until after some seminal event has occurred. In the realm of cyberspace, the challenge is magnified by the exponential pace of change in computational capabilities and the innovativeness of those who would use those capabilities for malicious intent. This is a challenge that may be difficult to

1 Reported in Federal Register. Vol. 78: No. 33. February 19, 2013. Part III: The President. Executive Order 13636 – Improving Critical infrastructure Cybersecurity.

2 Barak Obama, *Remarks by the President on Securing Our Nation's Cyber Infrastructure,* May 29, 2010, www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure (accessed February 17, 2013).

3 Jennifer Martinez, "White House Circulating Draft of Executive Order on Cybersecurity," *The Hill,* September 6, 2012, thehill.com/blogs/hillicon-valley/technology/248079-white-house-circulating-draft-of-executive-order-on-cybersecurity (accessed February 17, 2013).

4 Douglas Warfield (2012) "Critical Infrastructures: IT Security and Threats from Private Sector Ownership," *Information Security Journal: A Global Perspective*, 21(3):127–136.

5 Jennifer LeClaire, "Obama May Sign Cybersecurity Executive Order," *CIO Today,* November 16, 2012, www.cio-today.com/news/Obama-May-Sign-Cyber-Security-Order/story.xhtml?story_id=100003G6EP88 (accessed February 18, 2013).

surmount, given the slow nature of the legislative process. Cybersecurity is one of the most pressing national security issues confronting countries around the world. It can be broadly defined to incorporate several subtopics – including, but not limited to, Internet governance and jurisdiction, national security, and critical infrastructure protection. Gaps in cybersecurity can put individuals, business, and government at risk for a range of cyberattacks. The significant performance improvements witnessed over the last two decades in communication, hardware, software, and various types of user devices, coupled with decreasing costs, have made such technology – including a wide range of portable wireless devices that enable end-users to access information from anywhere at any time – more affordable and pervasive than ever before. Cybersecurity is loosely understood to be intended to protect against an array of threats often interchangeably identified as cybercrime, cyberattacks, and cyberterrorism. It has been suggested, however, that the nation would be better equipped to protect its critical infrastructure in cyberspace if cyberattacks were viewed as a matter of national defense, rather than as a criminal act with its slower investigative process and attendant legal procedures.[6]

Cybercrime, which costs organizations and individuals worldwide billions of dollars in losses every year, continues to be on the rise, and cybercriminals are launching increasingly sophisticated cyberattacks aimed at disrupting businesses by stealing personal information or by interrupting or suspending Internet services in what is known as denial-of-service (DoS) attacks. A DoS attack involves flooding a server with huge quantities of data (such as e-mails or server requests) until the server collapses. Cyberattacks have become a real threat to many businesses, national economies, and individual Internet users,[7] resulting in such devastating consequences as unavailable service, loss of productivity, loss of reputation, theft of intellectual property, and disruption of critical infrastructure operations. Cybersecurity law, termed as such, is rather novel, but there are existing laws, such as the Computer Fraud and Abuse Act (CFAA), that, while not historically coined "cybersecurity laws," are relevant to cybersecurity. In addition, many cybercrimes, such as individual identity theft, are often prosecuted under a variety of state and local criminal laws that may or may not have originally been

6 Sean Condron (2007)"Getting It Right: Protecting American Critical Infrastructure in Cyberspace," *Harvard Journal of Law & Technology*, 20(2):403–422. jolt.law.harvard.edu/articles/pdf/v20/20HarvJLTech403.pdf.

7 Benjamin J. Brooker, Jonathan Crawford, and Barry M. Horowitz, "A Framework for the Evaluation of State Breach Reporting Laws," in Proceedings of IEEE Systems and Information Engineering Design Symposium, April 2007; and Natalie Granado and Gregory White, "Cybersecurity and Government Fusion Centers," in Proceedings of the 41st Hawaii International Conference on System Sciences, 2008.

directly related to cybercrime but that, to the extent possible, have adapted to meet this new need.

There are several challenges inherent in the quest for better cybersecurity. First, the legal consequences for those involved directly or indirectly in cyberattacks are considered to be rather light, with judges often giving only a "slap on the wrist" to individuals who, for instance, simply write and sell malware/other malicious codes but are not involved in their launch.[8] Second, the anonymity that the Internet affords yields the problem of attribution (who is responsible for the act?), but to remove this "privilege" of anonymity could be construed as infringing upon the current freedom and privacy that the Internet provides. Third, the US public needs to be more aware of cyber vulnerabilities and threats and to understand its role in cybersecurity. And fourth, precision is needed in the definition of cybersecurity to distinguish between computer-related offenses that are a threat to national security and those that are not. The law is one mechanism for addressing these challenges. There are laws already in existence, but gaps in their coverage exist.

The history of cybersecurity law reflects a mix of legal areas and sources: cybercrime, cyber warfare, national security (protection of critical infrastructure), legislative statutes, and presidential directives.[9] The origins of cybersecurity law are somewhat less definitive. Some sources indicate that this body of law began in 1998, when former President Clinton issued Presidential Decision Directive 63 (PDD-63) addressing critical infrastructure protection.[10] However, the CFAA, which first became law in 1986, preceded PDD-63. Amending the Counterfeit Access Device and Abuse Act, which was passed in 1984, the CFAA (18 U.S.C. § 1030 *et seq.*) essentially states that whoever intentionally accesses a computer without authorization, or exceeds authorized access, and thereby obtains information from any protected computer, if the conduct involved an interstate or foreign communication, shall be punished under the act. In 1996 the CFAA was broadened by an amendment in which the term *protected computer* replaced the original term *federal interest computer*.[11]

---

8 Kimberly Peretti, "Cyber Criminals: Who Are They? Why Are They Successful? How Do We Respond?" presentation at SUMIT_11 Symposium, October 18, 2011, safecomputing.umich.edu/events/sumit11/.

9 Acklyn Murray, Sherali Zeadally, and Angelyn Flowers, "An Assessment of US Legislation on Cybersecurity," in Proceedings of the 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec 12), Kuala Lumpur, Malaysia, June 26–28, 2012.

10 Stephanie A. DeVos (2011) "The Google-NSA Alliance: Developing Cybersecurity Policy at Internet Speed," *Fordham Intellectual Property, Media and Entertainment Law Journal* 21(1):172–227, ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1280&context=iplj.

11 The Internet Law Treatise, 2012, ilt.eff.org/index.php/Computer_Fraud_and_Abuse_Act_(CFAA).

2 Overview of Current (Relevant) Laws and Agreements

Various types of threats are addressed by different categories of law. In addition, the inherent international nature of cyberspace often means that both domestic laws and international agreements/treaties are necessary to address cyberattacks and exploitations. The *2011 Data Breach Investigations Report* provides insight into the effectiveness of existing laws to address cybersecurity threats.[12] One of the major recommendations of that report essential to increasing information security is increased data sharing among the various systems used in providing cybersecurity as a means of encouraging businesses to share data. Existing laws such as the Critical Infrastructure Information Act (6 U.S.C.A § 133 *et. seq.*) have provisions that limit how the federal government can use data provided by businesses. Section 2 below describes legislation that, had it been enacted by the 112th Congress, would have modified that limitation in an effort to enhance cybersecurity.

The CFAA, addressing fraud and related activity in connection with computers, is the most significant law to date in the US to address cybersecurity. Since being enacted in 1986, it has undergone several modifications, the latest being in 2008.[13] According to a Congressional Research Service (CRS) report, "The federal computer fraud and abuse statute, 18 U.S.C. 1030 [*sic*], outlaws conduct that victimizes computer systems. It is a cybersecurity law. It protects federal computers, bank computers, and computers connected to the Internet. It shields them from trespassing, threats, damage, espionage, and from being corruptly used as instruments of fraud. It is not a comprehensive provision, but instead it fills cracks and gaps in the protection afforded by other federal criminal laws."[14] Providing an overview of the CFAA, the CRS report discusses the offenses covered under the act, other *traditional* crimes and laws related to CFAA offenses, and ways in which *traditional* laws may also be leveraged to prosecute cyber offences. The cyber offenses covered in the report are trespassing in government cyberspace, obtaining information by unauthorized computer access, causing computer damage,

12 Wade Baker et al., *2011 Data Breach Investigations Report* (Verizon, May 6, 2012), 67, www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf (accessed February 15, 2013).

13 The Internet Law Treatise, 2012.

14 Charles Doyle, *Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws* (Washington, D.C.: Congressional Research Service, Library of Congress, December 2010), 2, www.fas.org/sgp/crs/misc/97-1025.pdf.

engaging in computer fraud, making extortion threats, trafficking in computer access, and conducting computer espionage. "[The CFAA] deals with computers as victims; other laws deal with computers as arenas for crime or as repositories of the evidence of crime or from some other perspective. These other laws – laws relating to identity theft generally, obscenity, pornography, gambling, inter alia" – are covered by other statutes.[15]

The CFAA enables the US Attorney's Office to prosecute computer hacking offenses, fraud and related activity in connection with computers, and intentional unauthorized access into a protected computer that causes damage in excess of $5,000.[16] And there are other laws as well that protect against crimes committed in cyberspace. For example, intellectual property crimes or theft-of-information crimes are prosecuted under Title 18, U.S.C. § 2319 (criminal infringement of a copyright), § 2320 (trafficking in counterfeit goods/trademark violations), and § 1832 (theft of trade secrets).[17]

While the domestic laws in the US that can address cyber-related offenses are numerous and are maturing over time, there is concern about the efficacy of these laws given the inherently global nature of cyberspace. The US has adopted laws defining as criminal various forms of conduct, including improper intrusion into and deliberate damage of computer systems. Unfortunately, such laws have little effect on individuals, groups, or governments over whom the US lacks – or is unable to secure – regulatory or criminal jurisdiction: "The current, largely unilateral and defensive measures relied upon to provide cybersecurity in the U.S … are widely viewed as insufficient to ensure an adequate level of safety."[18] There are some international treaties and agreements that can have more impact than the US domestic law alone. For instance, the Council of Europe Convention on Cybercrime, a treaty ratified by the US in September 2006,[19] addresses both cyberattacks and cyber exploitation.

---

15 Ibid., 6.

16 Wayne Arnold, "TECHNOLOGY; Philippines to Drop Charges on E-Mail Virus," *New York Times*, August 22, 2000, www.nytimes.com/2000/08/22/business/technology-philippines-to-drop-charges-on-e-mail-virus.html (accessed February 17, 2013).

17 Ibid.

18 Abraham Sofaer, David Clark, and Whitfield Diffie, "Cyber Security and International Agreements," in *Proceedings of Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for US Policy* (Washington, D.C.: National Academy of Sciences, 2009), 187, www.cs.brown.edu/courses/csci1950-p/sources/lec17/Sofaer.pdf.

19 Council of Europe, Convention on Cybercrime CETS No.: 185 (May 6, 2012), www.conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=28/12/2011&CL=ENG.

3 US Federal Legislative Activity

This section provides an overview of the extent to which the 112th Congress tried to address the challenges presented earlier. When viewed comprehensively, the legislation presents a patchwork of often overlapping goals and strategies for improving US cybersecurity. In addition to the legislation proposed by the White House, over twenty bills relating to some aspect of cybersecurity were introduced in the Senate and House of Representatives during the first half of the 112th Congress (from January 5, 2011 to January 3, 2012). These bills addressed cyberattacks, cyber exploitation, and protection of intellectual property.

3.1 Proposed Legislative Changes

The focus areas of the proposed legislation submitted by the White House to the 112th Congress included: Protecting the American people, protecting the nation's infrastructure, protecting federal government computers and networks, and creating new frameworks to protect individuals' privacy and civil liberties.[20] One of the most significant parts of that legislation was the National Data Breach Notification law. No such law currently exists, and each state is responsible for enacting breach notification statutes, although doing so is not yet required. Therefore, an individual's expectation of notification – for example, when his or her personal information is obtained from the local grocery store or a newspaper subscription through a computer breach – varies according to where that person lives. The White House proposals included provisions for enhanced criminal penalties; notification of data breaches to enhance consumer protection; increased responsibility for the Department of Homeland Security in the cybersecurity arena; establishment of a regulatory framework for critical infrastructure; establishment of baseline standards for federal computing systems; and improved cybersecurity manpower training. More importantly, these proposals may be predictive of what will be important to the second Obama administration.

Tables 1 and 2 present a summary of the cybersecurity-related legislation proposed in the Senate and the House of Representatives, respectively, during the 112th Congress. Included with each bill is the date of the latest major action as of the end of federal fiscal year 2012 (September 30). Dates followed by an asterisk indicate that the latest action taken was on the same day that the legislation was introduced. These tables illustrate the breadth and diversity of the

20 White House, "FACT SHEET: Cybersecurity Legislative Proposal," press release, May 12, 2011, www.whitehouse.gov/the-press-office/2011/05/12/fact-sheet-cybersecurity-legislative-proposal.

Table 1 112th Congress: Senate Proposed Bills.[21]

Bill #	Name of legislation	General purpose
S.21	Cyber Security and American Cyber Competitiveness Act of 2011	To enhance American information technology industries and secure sensitive information on American citizens and businesses.
	1/25/11*	[Referred to the Committee on Homeland Security & Governmental Affairs]
S.372	Cybersecurity and Internet Safety Standards Act	To develop and enforce voluntary or mandatory-minimum cybersecurity and Internet safety standards for users based on cost-benefit analysis.
	2/16/11*	[Referred to the Committee on Commerce, Science & Transportation]
S.413	Cybersecurity and Internet Freedom Act of 2011	To amend the Homeland Security Act of 2002 and a series of laws so as to enhance the security and resiliency of the US communications infrastructure and close gaps in current law.
	5/23/11	[Referred to the Committee on Homeland Security & Governmental Affairs: hearings held]
S.813	Cyber Security Public Awareness Act of 2011	To inform US residents of cyberthreats that affect the public, the government, businesses, and other critical infrastructure using measurable statistics.
	4/13/11*	[Referred to the Committee on Homeland Security & Governmental Affairs]
S.968	Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011	To prevent online threats to economic creativity and theft of intellectual property with international cooperation.
	1/23/12	[Action taken by the Judiciary Committee: subsequently presented to the Senate for a vote and withdrawn by unanimous consent of the Senate.] (This was the Senate version of the Stop Online Piracy Act H.R. 3251, also known as SOPA, discussed below)
S.1151	Personal Data Privacy and Security Act of 2011	To mitigate identity theft; ensure privacy; provide notice of security breaches; and enhance criminal penalties, law enforcement assistance, and other protections against security breaches, fraudulent access, and misuse of personally identifiable information.
	11/7/11	[Action taken by the Judiciary Committee: written reports by the Committee, Additional, and Minority reports filed]

21 *OpenCongress.com*, May 6, 2012, www.opencongress.org/; Library of Congress, www.thomas.loc.gov.

(**Table 1** Continued)

Bill #	Name of legislation	General purpose
S.1152	Cybersecurity Enhancement Act of 2011	To address the need for further advancements in cybersecurity research, development, and technical standards as relates to establishing and enforcing security standards to reduce system vulnerabilities in government systems.
	6/7/11	[Referred to the Committee on Commerce, Science & Transportation]
S.1159	Cyberspace Warriors Act of 2011	To require the study of recruitment, retention, and development of cyberspace experts to assist in current laws or policies ensuring cybersecurity.
	6/8/11*	[Referred to the Committee on Armed Services]
S.1207	Data Security and Breach Notification Act of 2011	To enable protections for consumers by requiring limited security policies and procedures to protect data containing personal information, and to provide for nationwide notice in the event of a security breach.
	6/15/11*	[Referred to the Committee on Commerce, Science & Technology]
S.1408	Data Breach Notification Act of 2011	To require federal agencies and persons engaged in interstate commerce, in possession of data containing sensitive personally identifiable information, to disclose any breach.
	2/6/12	[Committee on the Judiciary: Placed on Senate Legislative Calendar No. 316 under General Orders]
S.1469	International Cybercrime Reporting and Cooperation Act	To require the reporting of the capacity of foreign countries to combat cybercrime, to develop action plans to improve that capacity, and to offer financing to encourage foreign compliance.
	8/2/11*	[Referred to the Committee on Foreign Relations]
S.1535	The personal data protection and breach accountability act of 2011	To protect consumers by mitigating the vulnerability of personally identifiable information, providing notice and remedies in the wake of breach, and holding companies accountable for prevention; also, to enhance criminal and civil penalties.
	9/22/11	[Action taken by Committee on the Judiciary Committee; subsequently placed on Senate Legislative Calendar No. 182 under General Orders]
S.2105	Cybersecurity Act of 2012	To reduce the private sector's inadequate cybersecurity protections by offering incentives to develop and promote self-protection standards.
	8/2/12	[Defeated by the Senate.]

(**Table 1** Continued)

Bill #	Name of legislation	General purpose
S.2151	SECURE I	To improve information security by strengthening and enhancing cybersecurity by using research, education, information, and technology. The bill highlights cyberthreat information sharing, coordination of policies, increased criminal penalties, and increased research and development.
	3/1/12	[Referred to the Committee on Commerce, Science & Technology]

Table 2 112th Congress: House Proposed Bills.[22]

Bill #	Name of legislation	General purpose
H.R. 76	Cyber Security Education Act	To authorize the secretary of the Department of Homeland Security to establish a program for institutions of higher education expansion in cybersecurity professional development.
	2/25/11	[Referred to the Committee on Higher Education & Workforce Development]
H.R.96	Internet Freedom Act	To prohibit additional regulation of the Internet by the Federal Communications Commission.
	2/1/11	[Referred to the Committee on Communications & Technology]
H.R.174	Homeland Security Cyber and Physical Infrastructure Protection Act	To amend the Homeland Security Act of 2002 so as to enhance domestic preparedness by establishing a Cybersecurity Compliance Division and authorizing the Department of Homeland Security to enhance cyber and physical infrastructures.
	2/8/11	[Referred to the Committee on Technology, Information, Policy, Intergovernmental Relations & Procurement Reform]
H.R.1136	Executive Cyberspace Coordination Act of 2011	To address security standards for government and critical infrastructure systems through a regulatory framework for critical infrastructure and other measures to assist enforcement of security standards to reduce vulnerabilities.
	4/1/11	[Referred to the Subcommittee on Government Organization, Efficiency & Financial Management]

22 *OpenCongress.com*, May 6, 2012, www.opencongress.org/; Library of Congress, www.thomas.loc.gov.

(**Table 2** Continued)

Bill #	Name of legislation	General purpose
H.R.2096	Cybersecurity Enhancement Act of 2011	To extend cybersecurity research, development, and technical standards in security systems.
	5/7/12	[Referred to the Committee on Commerce, Science & Transportation]
H.R.3261	Stop Online Piracy Act	To increase penalties for cyber exploitation of US intellectual property with international and foreign entity provisions; to coordinate with foreign governments to prevent piracy of US assets.
	12/16/11	[Committee on the Judiciary, Subcommittee on Intellectual Property: committee consideration and mark-up sessions held] (As noted above, the Senate version of this legislation, S.968, was withdrawn.)
H.R.3523	Cyber Intelligence Sharing and Protection Act (CISPA) of 2011	To modify Title XI of the National Security Act of 1947 so as to encourage private companies to share cybersecurity-related information with the US National Security Agency, limiting liability with regard to the sharing of personal information.
	4/26/12	**[Passed by the House of/Representatives]**
	5/7/12	(Referred to the Senate Select Committee on Intelligence)
H.R.3674	PRECISE Act of 2011	To amend the Homeland Security Act of 2002 to make certain improvements in the laws relating to cybersecurity, and for other purposes.
	9/12/12	[Considered by six committees: Homeland Security; Oversight & Government Reform; Science, Space, & Technology; Judiciary; Permanent Select Intelligence; and Energy & Commerce] [Placed on the House Union Calendar, No. 501]
H.R.3834	Advancing America's Networking and Information Technology Research and Development Act of 2012	To amend the High-Performance Computing Act of 1991 to authorize activities for support of networking and information technology research.
	5/7/12	[Referred to the Senate]
		(Senate received and referred to the Senate Committee on Commerce, Science, and Transportation)

(**Table 2** Continued)

Bill #	Name of legislation	General purpose
H.R.4527	Federal Information Security Amendments Act of 2012	To amend the Federal Information Security Management Act of 2002 to improve the security of federal information technology systems; to require the continuous monitoring of computer systems and provide the Office of Management and Budget and federal agencies with specific new responsibilities to secure federal information systems
	5/2/12	[Referred to the House Subcommittee on Trade]
H.R.4263	SECURE IT Act of 2012	To equip and develop effective cybersecurity regulations and regulatory processes to develop rules and standards applicable to the dynamic cyber-domain.
	4/19/12	[Referred to the House Subcommittee on Crime, Terrorism, and Homeland Security]

proposed cybersecurity legislation. However, they also reveal that the overwhelming majority of these bills never made it out of committee. It is worth considering how much of the difficulty in legislatively addressing cybersecurity is attributable to the number of different committees involved. For instance, in the Senate, fourteen pieces of legislation were considered by five different committees; in the House, ten bills were referred to seven different committees or subcommittees, with one bill alone referred to six different committees. One key fact, illustrated by the range of committee assignments, is the extent to which cyberspace and its protection have become a ubiquitous part of daily life. Unfortunately, despite the array of cybersecurity legislation introduced and considered during the 112th Congress, any legislation still pending at the adjournment of a congressional session dies and, if it is to be reconsidered, must be reintroduced in the next session.

Of all the cybersecurity legislation introduced in 2011, the Cyber Intelligence Sharing and Protection Act (CISPA) was the most significant and potentially far-reaching to be considered by Congress. The unrestricted flow of information to the National Security Agency and the use of shared information for purposes unrelated to cybersecurity (e.g., ordinary law enforcement), as authorized by CIPSA, caused significant concerns among privacy advocates.[23] Critics of CISPA

23 Leigh Beadon, "Did CISPA Actually get *Better* Before Passing? Not Really," *Techdirt,* April 27, 2012, Cwww.techdirt.com/articles/20120427/08375418687/did-cispa-actually-get-better-before-passing-not-really.shtml (accessed February 16, 2013).

had four major objections: (1) the overly broad definition of information that could be shared with government agencies, irrespective of privacy or other laws; (2) the "sharing" it called for, which could lead to an expanded government role in the monitoring of private communications; (3) a shift in the control of government cybersecurity activities from civilian agencies to the military; and (4) the fact that, once shared, information could be used for any purpose not specifically prohibited, regardless of whether it was related to cybersecurity.[24]

Having moved to the Senate, CISPA did not make it out of the Senate Select Committee on Intelligence. Competing against CISPA in the Senate was the Lieberman-Collins Cybersecurity Act of 2012, which, like CISPA, also permitted Internet service providers (ISPs) to share information with the government without a warrant. Unlike CISPA, however, the Cybersecurity Act of 2012 contained protection for the nation's critical infrastructure systems.[25] While CISPA provoked extensive outcry from privacy advocates, the Cybersecurity Act provoked equally intense outcry from business lobbyists, who argued that any safety standards would be an unfair costly burden for industry.[26] Despite its sponsors' concession to Republican lawmakers to change the proposed regulatory requirements from mandatory to voluntary, the Cybersecurity Act was six votes short of the required 60 votes needed to break a Republican filibuster. It has been estimated that about 85% of the nation's critical infrastructure is owned or operated by the private sector.[27] Therefore, gaps in the protection of this sector leave the nation vulnerable. This point was glaringly illustrated less than two months after the legislation was defeated: in September 2012, within the space of slightly more than one week, five major US banks were hacked, resulting in online access problems for customers and distributed denial-of-service (DDoS) attacks.[28] A more advanced

24 Andrew Couts, "Watch Out Washington: CISPA Replaces SOPA as Internet's Enemy No. 1," *Digital Trends,* April 5, 2012, www.digitaltrends.com/web/watch-out-washington-cispa-replaces-sopa-as-internets-enemy-no-1/ (accessed February 16, 2013).

25 Donny Shaw, "White House Indicates Support for Cybersecurity Bill That Includes CISPA-Like Language," *OpenCongress,* May 4, 2012, www.opencongress.org/articles/view/2490-White-House-Indicates-Support-for-Cybersecurity-Bill-Thta-Includes-CISPA-Like-Language (accessed February 16, 2013).

26 Gerry Smith, "Cyber Security Law Fails to Pass Senate before Month-Long Break," *Huffington Post*, August 2, 2012, www.huffingtonpost.com/2012/08/02/cyber-security-law_n_1733691.html (accessed February 16, 2013).

27 US Department of Homeland Security, "Critical Infrastructure Sector Partnerships" (n.d.), www.dhs.gov/critical-infrastructure-sector-partnerships.

28 Chris Zoladz, "US Bank, PNC Hacked, Report Website Problems," *WZZM13.com,* September 27, 2012, www.wzzm13.com/news/article/226840/14/US-Bank-PNC-hacked-report-website-problems (accessed February 16, 2013).

DoS attack, a DDoS attack is one in which more than one computer is used to send the data or requests to the server. Often, the computers being used to send data in DDoS attacks are unaware that they have, in essence, been hijacked.

3.2 US Cybersecurity Legislation and the Limitations of National Borders

Assuming the existence of legislation, the biggest hurdle to US efforts in protecting its cyberspace is the global nature of cyberspace and jurisdictional issues. A court cannot try a case simply because an offense has occurred that, under US law, is defined as a crime. A court must also have jurisdiction by virtue of the offense having occurred within that court's geographic boundaries. But to prosecute a case, either the offender must be within the court's geographic boundaries or there must be a legally prescribed mechanism to bring the offender within those boundaries.

The notion of double criminality, an international legal concept connected to international jurisdiction issues, requires that the criminal act in the aggrieved nation share the related criminal code on that same conduct in the host nation in order for extradition of the offender to the aggrieved nation to be permissible.[29] On paper this sounds fairly simple; however, in the challenges of international relations and national sovereignty, things are never as simple as they may appear. The Philippines' Cybercrime Prevention Act of 2012 illustrates the importance of appropriately labeling behavior as criminal. Approved on September 12, 2012, the Cybercrime Prevention Act was devised specifically to address the Philippines' porous cybersecurity laws, which had the effect of creating a cyber-safe haven.[30] It effectively closed a decade's-old gap in Philippine law that failed to criminalize crimes committed on computers. Had the act been in effect in 2000, for example, it would have permitted the prosecution of Onel de Guzman, creator of the infamous "Love Bug" virus that affected millions of computer users worldwide and caused significant financial damage. But Mr. Guzman could not be charged or extradited because, at the time of his action, launching a virus did not constitute a crime under Philippine law.[31]

---

29 US Department of Justice, Computer Crime and Intellectual Property Section Criminal Division, *Prosecuting Computer Crimes* (Washington, D.C.: Office of Legal Education, n.d.), www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf.

30 Mehzabin Sultana, "CyberCrime Prevention Act of 2012 Approved by Congress," *Latest Digitals*, May 29, 2012, www.latestdigitals.com/2012/05/29/cybercrime-prevention-act-of-2012-approved-by-congress/ (accessed February 16, 2013).

31 Arnold, "TECHNOLOGY; Philippines to Drop Charges on E-Mail Virus."

Hacking into the Pentagon's computer networks, on the other hand, is clearly a crime and has been for some time. However, after initial agreement, the extradition of a British computer hacker sought by the US under an extradition order dating back to 2006 was denied in October 2012.[32] Gary McKinnon admitted hacking into 97 Department of Defense and National Aeronautics and Space Administration (NASA) computers while looking for evidence of unidentified flying objects from his London apartment.[33] While the British government cited human rights concerns, suggesting that the defendant's Asperger's syndrome and depression would make him a suicide risk if he were sent to the US, there has also been growing British opposition to the extradition treaty involved, which was signed in 2010 by the UK and the US. British critics allege that the treaty has three serious deficiencies: (1) the outsourcing of British judicial responsibilities to the US, (2) the lack of reciprocal benefits from the US, and, most importantly, (3) the failure to distinguish between serious and lesser offenses.[34] These critics argue that this legislation was "designed to help prosecute terrorists but ... has been misused by American prosecutors as a catchall measure in less onerous cases unrelated to national security."[35] Despite these criticisms, it is clearly arguable that penetrating Pentagon and NASA computer networks could be considered a threat to the US national security. This example suggests that even the existence of international criminal laws, treaties, and compacts does not completely resolve jurisdictional questions.

The US has an easier time crossing international boundaries when the theft of intellectual property is at issue. One instance in which a US court found jurisdiction over the computer servers and then used that jurisdiction to reach defendants located in other countries is the controversial Megaupload case. In January 5, 2012, the file-sharing website megaupload.com (a Hong Kong-based company) was shut down by the Federal Bureau of Investigation (FBI) as its owners were charged in a five-count indictment in the US District Court for the Eastern District of Virginia. The charges were

1. Conspiracy to commit racketeering: violation of 18 U.S.C. § 1962(d)
2. Conspiracy to commit copyright infringement: violation of 18 U.S.C. § 371.
3. Conspiracy to commit money laundering: violation of 18 U.S.C. § 1956(h).

---

32 Alan Cowell and John F. Burns, "Britain Refuses to Extradite Computer Hacker Sought in U.S.," *New York Times,* October 16, 2012, www.nytimes.com/2012/10/17/world/europe/britain-refuses-to-extradite-computer-hacker-sought-in-us.html?_r=0 (accessed February 16, 2013).

33 Mark Tran, "Extradition of Computer Hacker Gary McKinnon Put on Hold," (UK)*Guardian,* May 29, 2010, www.guardian.co.uk/world/2010/may/20/computer-hacker-gary-mckinnon-extradition-on-hold (accessed February 17, 2013).

34 Cowell and Burns, "Britain Refuses to Extradite Computer Hacker."

35 Ibid.

4. Criminal copyright infringement by distributing a copyrighted work being prepared for commercial distribution on a computer network & aiding and abetting of criminal copyright infringement: violation of 18 U.S.C. §§ 2 and 2319 and of 17 U.S.C. § 506.
5. Criminal copyright infringement by electronic means & aiding and abetting of criminal copyright infringement: violation of 18 U.S.C. §§ 2 and 2319 and of 17 U.S.C. § 506.[36]

The US Department of Justice reported seizing 18 domains associated with megaupload.com, executing more than 20 search warrants in more than eight countries, and seizing over $50 million in assets.[37] At the time of the shutdown, megaupload.com controlled 565 servers in Virginia and 630 in the Netherlands, as well as others around the world.[38] Four of the defendants who were arrested and charged in a New Zealand courtroom and are currently contesting extradition to the US are Dutch citizens. Others eventually arrested include another Dutch citizen and two German citizens.[39] The significance of this case is that by using *existing* laws, the US, in a far-reaching move, was able to shut down a foreign company as well as instigate the arrest and potential trial of foreign nationals. The US government primarily relied on traditional conspiracy and racketeering laws, coupled with the more recent Digital Millennium Copyright Act of 1998. The US District Court for the Eastern District of Virginia based its jurisdiction on the fact that megaupload.com leased server space from a company headquartered in the Eastern District of Virginia using 525 computer servers also located in that district.[40] For some, this was an indication that more far-reaching laws that had been under consideration by the 112th Congress, such as the Stop Online Piracy Act (SOPA), were unnecessary.

This case is still unresolved. While megaupload.com was shut down and its owners are currently facing charges in a federal court, the case has not yet gone to trial. Even if the defendants are convicted, this is a case that will likely spend

36 US District Court for the Eastern District of Virginia, *USA v. Kim Dotcom, Megaupload Limited, et al.,* "Indictment," January 5, 2012, www.washingtonpost.com/wp-srv/business/documents/megaupload_indictment.pdf.

37 David Kravets, "Feds Shutter Megaupload, Arrest Executives," *Wired,* January 19, 2012, www.wired.com/threatlevel/2012/01/megaupload-indicted-shuttered/ (accessed February 16, 2013).

38 Nate Anderson, "Why the Feds Smashed Megaupload," *Ars Technica,*January 19, 2012, arstechnica.com/tech-policy/2012/01/why-the-feds-smashed-megaupload/ (accessed February 16, 2013).

39 Nick Perry, "Popular File-Sharing Site Megaupload Shut Down," *USA Today,*January 20, 2012, www.usatoday.com/tech/news/story/2012-01-19/megaupload-feds-shutdown/52678528/1 (accessed February 16, 2013).

40 *US District Court, USA v. Kim Dotcom,*"Indictment."

years being litigated and appealed. In other words, it has yet to be seen whether existing laws are sufficient for conviction and the upholding of that conviction. If they are not, an argument can still be made that new and stronger laws are necessary to protect against the theft of US intellectual property. More significant for the future of Internet privacy in the US is the distinction that the FBI made in this case between "physical" data and "digital" data when the bureau copied the content on Megaupload's foreign servers and brought the digital copies back to the US. The FBI acknowledged that it would not have been permissible for the Bureau to copy "physical" documents.[41]

In another incident, the Ukrainian government shut down the bit torrent site "Demonoid," raiding its offices and sealing the company's servers after copying the information on them. No one was arrested because Demonoid, as a tracker site rather than a host site, had not committed a criminal violation under Ukranian law.[42] It was reported but not confirmed that the action taken by the Ukrainian government was scheduled to coincide with the visit of the Ukrainian Deputy Prime Minister to the US; on the agenda for that meeting was copyright infringement, and the Ukrainian government was rumored to be eager to demonstrate its willingness to cooperate.[43] It should be noted that this is an example of a situation where no law in the host country was violated. Yet this particular theft of US intellectual property was terminated. In this instance, the US reacted to the violation of its law by allegedly letting the host government seize the offending instrumentalities, even though the behavior did not violate the law of that host country.

4 Cybersecurity Legislation Worldwide

Cyberspace is global, and enhancing cyber security requires an active, multilayered international engagement strategy to work aggressively to combat cybercrime. Improving cooperation against cyberterrorists and hackers, and creating

41 "FBI Accused over Removal of Megaupload Data," *BBC News*, June 7, 2012, www.bbc.co.uk/news/technology-18352289 (accessed February 16, 2013).

42 Daniel Ionescu, "Demonoid Torrent Site Gets Shut Down by Authorities," *PC World*, August 8, 2012, www.pcworld.com/article/260572/demonoid_torrent_site_gets_shut_down_by_authorities.html (accessed February 16, 2013).

43 Enigmax, "Demonoid Busted as a Gift to the United States," *TorrentFreak*, August 6, 2012, torrentfreak.com/demonoid-busted-as-a-gift-to-the-united-states-government-120806/ (accessed February 16, 2013).

broad international policies to assist in securing Internet activity, is key.[44] US Deputy Defense Secretary William J. Lynn III disclosed that in March 2011, computer hackers penetrated the network of an unnamed defense contractor and stole 24,000 sensitive files.[45] Lynn blamed the theft on a foreign power, although computer security experts claim that such missions are often contracted by foreign spy agencies to cyber criminals, who crack the security of both government computers and corporate networks at frequencies that are alarming. To meet the challenge posed by the new kinds of cybercrimes made possible by Internet-based technologies, many countries have reviewed their domestic criminal laws so as to deter computer-related crimes.[46] Some of these countries are Argentina, Australia, Austria, Canada, Denmark, Finland, France, Germany, Greece, India, Italy, Japan, Malaysia, Portugal, Singapore, Spain, Sweden, Switzerland, Turkey, and the UK.[47] However, no country has fully resolved all the issues associated with cybercrime, and the legislation enacted by different countries cover only a few of the classified computer-related offenses. As new types of cyberattacks continue to emerge with these dynamic and fast-changing technologies, legislative actions will follow – albeit more slowly. Different nations have responded differently to this problem. Brief descriptions of a few international efforts are presented below.

4.1 Europe

4.1.1 European Union (EU)

To ensure Europe's welfare and competitiveness, the EU ranks cybersecurity as one of its high priorities. A recent survey among EU citizens revealed that 29% are not confident enough to use the Internet for banking transactions and online purchases and that 12% have been the victims of online fraud.[48] To enable its citizens to continue to reap the benefits of cyberspace and protect it, the EU has

44 The White House, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (Washington, D.C., May 2011), www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

45 Thom Shanker and Elisabeth Bumiller, "Hackers Gained Access to Sensitive Military Files," *New York Times*, July 14, 2011, www.nytimes.com/2011/07/15/world/15cyber.html?pagewanted=all (accessed February 16, 2013).

46 Mike Redford, "US and EU Legislation on Cybercrime," in Proceedings of the European Intelligence and Security Informatics Conference, Athens, Greece, September 12–14, 2011.

47 Cyber Crime Law, May 6, 2012, www.cybercrimelaw.net/Cybercrimelaw.html.

48 Catherine Ashton, "Cybersecurity: An Open, Free, Secure Internet," European Union External Action, October 4, 2012, www.eeas.europa.eu/top_stories/2012/081012_cyberspace_en.htm.

launched various initiatives to strengthen cybersecurity legislation and engage everyone with a stake in it – the private sector, government, society, international organizations, and individuals.[49] On September 11, 2012, the EU established the Computer Emergency Response Team (CERT-EU) to protect against cyberthreats.[50] CERT-EU is expected to play a fundamental role in developing a future comprehensive cybersecurity strategy and policy for the EU.[51] The EU Commission will also set up a European Cybercrime Center in 2013, to be located at The Hague;[52] the main goal of this center will be to coordinate national cybercrime authorities and develop training programs for future cybersecurity specialists. Currently, the EU's main challenge (similar to that of many countries) is the lack of notification of security breaches to authorities.[53] Many of these security incidents are still kept confidential or go unreported, making it difficult for policy makers to know about their actual impact, frequency, and causes.[54] To address this issue, the European Network and Information Security Agency (ENISA) will develop an EU framework that will require the notification of security breaches to the authorities.

4.1.2 United Kingdom

The UK passed laws against cybercrime targeting DoS attackers with punishments of up to 10 years in prison. The law clarifies Britain's Computer Misuse Act, which had not specifically addressed DoS attacks;[55] that act mentioned penalties only for modifying content on a computer without authorization. Both DoS and DDoS attacks are prosecuted under the same laws. According to the 2006 version of the

49 Ibid.

50 European Commission, "Cyber Security Strengthened at EU Institutions Following Successful Pilot Scheme," press release, September 12, 2012, europa.eu/rapid/press-release_IP-12-949_en.htm?locale=en.

51 CERT-EU, cert.europa.eu/cert/plainedition/en/cert_about.html.

52 Benjamin Fox, "Parliament Demands Single EU Voice on Cyber-Security," *EUObserver.com,* June 13, 2012, euobserver.com/creative/116606 (accessed February 16, 2013).

53 Nikolaj Nielsen, "EU Cybersecurity Legislation on the Horizon," *EUObserver.com,* May 11, 2012, euobserver.com/justice/116239 (accessed February 16, 2013).

54 Marnix Dekker, Christoffer Karsberg, and Barbara Daskala, "Cyber Incident Reporting in the EU: An Overview of Security Articles in EU Legislation," European Network and Information Security Agency (ENISA) (August 2012), www.thecre.com/fisma/wp-content/uploads/2012/08/Cyber-Incident-Reporting-in-the-EU_FINAL.pdf.

55 Ben Quinn, "Facebook Hacker Jailed for Eight Months," (UK) *Guardian,*February 17, 2012, www.guardian.co.uk/technology/2012/feb/17/facebook-hacker-glenn-mangham-jailed?INTCMP=SRCH (accessed February 16, 2013).

act, impairing the operation of any computer, preventing access to any program or data in a computer, and restricting the operation of any program on a computer are all crimes punishable with a maximum of 10 years in prison.

4.1.3 Sweden

The Swedish government has used the Intellectual Property Rights Enforcement Directive, which is based on an EU directive, to force ISPs to provide the personal details of suspected copyright infringers. Implemented in 2006, the law allows copyright holders to obtain a court order forcing ISPs to provide the Internet protocol addresses identifying which computers have been illegally sharing copyrighted material.[56]

4.2 Africa

4.2.1 South Africa

South Africa attempted to address cybercrime as far back as 2002, when its parliament enacted the Electronic Communications and Transactions Act.[57] This act comprehensively delineates offenses and allows for the prosecution of cybercrimes. However, recent cybercrime incidents such as the Postbank (part of the South African Post Office) heist,[58] in which cybercriminals withdrew close to US$5 million in 3 days, continues to exploit deficiencies (such as improperly configured or old intrusion detection systems) in the network and security systems.

4.2.2 Nigeria

Nigeria has tried to pass a broad-ranging series of laws against cybercrime. Six laws were placed before the country's parliament in 2011 to outlaw many forms

56 "Piracy Law Cuts Internet Traffic," *BBC News,* April 2, 2009, news.bbc.co.uk/2/hi/7978853.stm (accessed February 16, 2013).

57 Electronic Communications and Transactions Act, 2002, *Government Gazette Republic of South Africa,* No. 25 of 2002 (August 2002), www.info.gov.za/view/DownloadFileAction?id=68060.

58 Werner Swart and Mzilikazi Wa Afrika, "It Was a Happy New Year's Day for Gang Who Pulled Off ... R42m Postbank Heist," *Times Live,* January 15, 2012, www.timeslive.co.za/local/2012/01/15/it-was-a-happy-new-year-s-day-for-gang-who-pulled-off...r42m-postbank-heist (accessed February 16, 2013).

of Internet misuse, including spamming, online identity theft, and buying goods online using stolen credit card details.[59] As of January 2012, however, these activities were still permissible in Nigeria, whose only legislation on Internet crime – Article 419 of the Nigerian Criminal Code – bans advanced fee fraud (a confidence trick in which the target is persuaded to advance sums of money in the hope of realizing a significantly larger gain). Article 419 provides a statutory definition of the criminal offense of fraud, defining it in three classes: fraud by false representation, fraud by failing to disclose information, and fraud by abuse of position.

4.2.3 Kenya

Kenya recently amended the Kenya Communications Act of 2009 to mandate that the Communications Commission of Kenya and Kenya's national Information and Communication Technology (ICT) Regulatory Authority develop a secure national electronic transactions framework.[60]

4.3 South America

Cybercrime is becoming a massive problem in South America, costing some $93 billion in yearly losses to companies and banks.[61] According to reports, the countries of Brazil, Mexico, and, more specifically, Argentina have the largest Internet penetration per capita of all the South American nations. In Proyecto Amparo (Support Project), an investigation conducted by a group of IT experts, the topology of cybercrime is noted for escalating in a more complex and sophisticated fashion in Latin America. The data reveal that cyberattacks directed toward banks cost an average of $50,000 dollars, or $50–60 per affected account.

---

59 John Leyden, "Nigeria Fails to Enact Cyber Crime Laws," (UK) *Register,* April 1, 2011, www.theregister.co.uk/2011/04/01/nigeria_cybercrime_law_fail/ (accessed February 16, 2013).

60 *The Kenya Information and Communications Act, 2009* (Kenya: National Council for Law Reporting with the Authority of the Attorney General, 1998; rev. ed. 2009), www.cck.go.ke/regulations/downloads/Kenya-Information-Communications-Act-Final.pdf.

61 Rubén Aquino Luna, Jose Luis Chavez Cortez, Leonardo Vidal, et al., *Computer Security Incident Management Manual: Latin America and the Caribbean, 2009* (Montevideo, Uruguay: Amparo Project, 2010), www.proyectoamparo.net/files/manual_seguridad/manual_en.pdf.

4.4 Asia and Australia

4.4.1 Malaysia

The Malaysian government has established a separate agency called Cybersecurity Malaysia,[62] which operates under the Ministry of Science, Technology, and Innovation to provide cybersecurity-related services (including legislation and regulatory aspects, emergency response, risk assessment, and cyberthreat research) and to closely monitor threats to Malaysia's national security. In the context of this work, Cybersecurity Malaysia focuses on the nation's current legislative framework and determines whether current legislation is sufficient to address traditional crimes as well as cyber-specific crimes.[63] For those laws that are not sufficient to address the legal challenges in the cyber environment, various types of amendments have been recommended. It is worth pointing out that although Malaysia has enacted some computer security-related laws, most of those laws are aimed at preventing unauthorized access. The country still relies on traditional general laws to prosecute computer-related criminal acts such as fraud and forgery. To foster international cybersecurity cooperation, Cybersecurity Malaysia has recently started collaborations (through a memorandum of understanding) with the Japan Computer Emergency Response Team Coordination Center (JPCERT/CC) and the Australian CERT.

4.4.2 Australia

The US and Australia have decided to provide funding for new research and development for future cybersecurity improvements as part of a trilateral initiative that includes the UK.[64] The agreement is particularly focused on modern cyberthreats emanating from the Pacific region, specifically China.[65] It provides the US with

62 Cybersecurity Malaysia, www.cybersecurity.my/en/index.html.

63 Mohd Shamir B Hashim, "Malaysia's National Cyber Security Policy: Towards an Integrated Approach for Cybersecurity and Critical Information Infrastructure Protection (CIIP)," in Proceedings of the 2009 ITU Regional Cybersecurity Forum for Africa and Arab States, Tunis, Tunisia, June 4–5, 2009, www.itu.int/ITU-D/cyb/events/2009/tunis/docs/hashim-cybersecurity-malaysia-june-09.pdf.

64 "White House on U.S.-U.K. Cybersecurity Partnership," *IIP Digital*, March 14, 2012, iipdigital.usembassy.gov/st/english/texttrans/2012/03/201203142090.html#axzz1xKaFSLwT (accessed February 16, 2013).

65 "ANZUS Cyber Security Message Aimed at China," *ComputerWorld*, April 27, 2012, www.computerworld.com.au/article/422926/anzus_cyber_security_message_aimed_china/ (accessed February 16, 2013).

access to Australian military facilities and with joint training exercises between the two nations.[66]

A more in-depth study of cybersecurity legislation in Asia is beyond the scope of this paper.[67]

5 Continuing Challenges and Issues

5.1 Fast Technological Change

"The invention and adoption of digital technologies by more than a billion people worldwide has occurred over the span of a few decades";[68] this is in stark contrast to the centuries that elapsed between the development of the European printing press by Gutenberg and the availability of printed books to other than an elite few. The rapid expansion of these new technologies has often left the legal system lagging behind when responding to the criminality these technologies bring about.

For instance, on July 26, 1989, graduate student Robert Tappan Morris was indicted in the US under the original 1986 version of the CFAA for spreading the Internet's first intentional worm virus, infecting more than 6000 universities, research centers, and military facilities. Morris's punishment was a $10,050 fine, 400 hours of community service, and 3 years' probation.[69] In comparison, on September 8, 2011, under amended US prosecution and sentencing guidelines, the cyber offender in *USA v. Luis Mijangos,* having infected a hundred computers with the intent of obtaining personal data and later demanding sexually explicit videos from female victims in exchange for not distributing other images, was sentenced to 72 months of imprisonment for deliberate acts of cyber extortion from 13 victims.[70] Mijangos pleaded guilty in the Central District of California's

66 "White House on U.S.-U.K. Cybersecurity Partnership."

67 But see Microsoft Corporation, *Asia Pacific Legislative Analysis: Current and Pending Online Safety and Cybercrime Laws* (Microsoft Corporation, 2007), www.itu.int/ITU-D/cyb/cybersecurity/docs/microsoft_asia_pacific_legislative_analysis.pdf.

68 John Palfrey and Urs Gasser, *Born Digital: Understanding the First Generation of Digital Natives* (New York: Perseus Books Group, 2008) 3.

69 *US v. Morris,* 928 F.2d 504, 505 (2d Cir. 1991), www.nyls.edu/user_files/1/3/4/30/84/85/114/137/morris.pdf.

70 Federal Bureau of Investigation, Los Angeles Division, "Orange County Man Who Admitted Hacking into Personal Computers Sentenced to Six Years in Federal Prison for 'Sextortion' of Women and Teenage Girls," September 1, 2011, www.fbi.gov/losangeles/press-releases/2011/orange-county-man-who-admitted-hacking-into-personal-computers-sentenced-to-six-years-in-federal-prison-for-sextortion-of-women-and-teenage-girls.

federal court system to computer hacking and wiretapping, and was referred to the Immigration and Customs Enforcement Agency because of his immigration status. The only similarity between these two crimes is that they both involved computers. Robert Morris's worm infestation of universities, research centers, and especially military facilities would today most likely be considered offenses against national security, warranting more than the sentence imposed at that time. Luis Mijangos's crimes, on the other hand, despite their unsavory nature, do not rise to the level of a national security threat. Morris infected 6000 computers, Mijangos infected 100.

The juxtaposition of these two distinct cases occurring 20 years apart illustrates the manner in which expansion in the use of computers – morphing from mainframes used primarily by universities, research centers, and the military into personal computers used in offices, then in homes, and then in our pockets as handheld mobile devices – led to societal awareness of the extent to which individuals can be victimized by computers. The universal computer use that developed over this 20-year period spawned an environment in which crimes committed using computers began to be viewed as offenses against the public, giving rise to the expectation that these offenses could be handled in the law enforcement arena. This expectation, however, requires either the use and application of existing laws or the creation of new laws to meet new challenges. These are among the reasons why the executive branch of the US government has repeatedly urged for passage of stronger cybersecurity measures that include increasing the maximum sentence, specifically for acts that could endanger national security, to twenty years in prison.[71]

5.2 Ongoing Issues for Cyberlaw to Address

Despite its relatively new arrival in the legal arena, cyberlaw presents the same continuing necessity for American jurisprudence to balance safety with individual liberties and freedoms. Tilting the balance toward safety suggests that cyberlaw will be increasingly presented as a matter of national defense and security. It will need to focus on safeguarding the nation's critical infrastructure – for example, electrical grids and water supply stations, all of which are dependent

71 *Administration's White Paper on Intellectual Property Enforcement Legislative Recommendations* (March 2011), www.whitehouse.gov/sites/default/files/ip_white_paper.pdf; Gina Stevens and Jonathan Miller, *The Obama Administration's Cybersecurity Proposal: Criminal Provisions* (Washington, D.C.: Congressional Research Service, Library of Congress, July 29, 2011), www.fas.org/sgp/crs/misc/R41941.pdf.

on computer systems – from foreign nations and terrorists. In 2009 it was estimated that a new variant of malware enters cyberspace every 2.2 seconds.[72] This does not take into account the potential damage to US infrastructure that could be caused by a Stuxnet-type worm or a Flame-type virus. Despite the necessity of protecting critical infrastructure, however, any such effort is difficult because of the requirement for legislative action and increased regulation. With 85% of the nation's critical infrastructure in the hands of the private sector,[73] increased regulation becomes a "hot button" political issue instead of a national security issue.

5.3 Unaddressed Challenges

An area of research not addressed in this article is the identification of future cybersecurity and legislative activity. The legislative process is often seen as slow, a perception that fails to take into account the deliberative nature of the process. The difficulty is that computer technologies change so quickly that legislation will always lag behind both the change and the harm it can cause. In the US the legislative process must coexist with constitutional requirements that laws be neither so vague that they infringe on otherwise protected activity under the First Amendment,[74] nor so broad that the average citizen is unable to determine what conduct is required or prohibited.[75] A more subtle contributing factor is that laws and policies tend to be developed by "digital immigrants," as distinct from "digital natives." Digital natives, generally defined as those born after 1980, are the first generation to be born and raised in a world of digital technologies.[76] Digital immigrants, on the other hand, have had to learn to adapt to that which may seem innate to a digital native. Like many immigrants, digital immigrants are navigating in territory that is foreign to them, which in some instances limits their ability to predict or anticipate cybersecurity needs before such needs occur.

---

72 Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do about It* (New York: Harper Collins, 2010).

73 Todd A. Brown (2009) "Legal Propriety of Protecting Defense Industrial Base Information Infrastructure," *Air Force Law Review* 64:211–237.

74 *Connally v. General Construction Co.*, 269 US 385 (1926), supreme.justia.com/cases/federal/us/269/385/case.html.

75 *Broadrick v. Oklahoma et al.*, 413 US 601 (1973), law.justia.com/lawsearch?query=Broadrick%20et%20al.%20v.%20Oklahoma%20et%20al.%2C%20413%20U.S.%20601%20%281973%29&dataset=supreme-court.

76 Palfew and Gasser, *Born Digital;* Michael Robinson (2008) "Digital Nature and Digital Nurture: Libraries, Learning and the Digital Native," Library Management 29(1/2):67–76. www.lib.cuhk.edu.hk/conference/aldp2007/programme/aldp2007_full_paper/MichaelRobinson.pdf.

It is essential that policy makers and the public understand that with the creation of new cybersecurity laws, entanglements in new moral hazards will intensify.[77] Arguments will continue to be raised regarding the constitutionality of possible reductions of privacy rights or of actions to censor content deemed "dangerous" speech on the Internet. These contradictions are predictable hurdles when confronting the development of cybersecurity policy. The passage of legislation that encourages companies to share cybersecurity data with the government by offering them antitrust protection can also result in the disclosure of personal data unrelated to national security, which may then lead to law enforcement investigations for other crimes. For instance, many individuals who visited file-sharing sites that have since been shut down by the government are concerned that their identities may be revealed and that they may be subject to prosecution or civil lawsuits. The Motion Picture Association of America (MPAA) is considering suing Megaupload users for copyright infringement – although after making this statement, the MPAA denied that that was its intent.[78] This is not merely an idle concern. In 2009, the Recording Industry Association of America brought a $669,000 civil suit against Joel Tenenbaum, a Boston University student, for illegal "sharing" on a peer-to-peer network ($22,500 per illegally downloaded and shared song). A lower court federal judge ruled the compensation "unconstitutionally excessive," but the First US Circuit Court of Appeals reinstated the penalty, leading to a plea before the US Supreme Court. On May 21, 2012, the Court upheld the verdict against Joel Tenenbaum. This also was a pre-SOPA case.

Nor have we addressed the adequacy or inadequacy of laws protecting individuals from identity theft and, more importantly, prosecuting those who have stolen others' identities. This is because identity theft is generally prosecuted at the state and local levels under their laws. As a result, there are great disparities in how identity theft is handled from one jurisdiction to another. Efforts to address cybersecurity regulations in the future will continue to be confronted by the fact that while individuals want to be protected against identity theft and persons "hacking" into their bank accounts, many are also disquieted by government penetration of what they consider their personal information despite its location on a computer server somewhere else. On the corporate side, while there is great concern for protecting intellectual property, there is also great concern

77 Stefan Fafinski (2011) "Public Policy Responses to Cybercrime," *Policy and Internet* 3(2), www.psocommons.org/cgi/viewcontent.cgi?article=1139&context=policyandinternet.

78 Mike Masnick, "MPAA Asks for Megaupload Data to be Retained so It Can Sue Users ... Then Insists It Didn't Really Mean That," *Techdirt*, March 21, 2012, www.techdirt.com/articles/20120321/12073218187/mpaa-asks-megaupload-data-to-be-retained-so-it-can-sue-users-then-insists-it-didnt-really-mean-that.shtml (accessed February 17, 2013).

about being subjected to increased government regulations, even when those regulations are designed to protect the consumers whom the companies serve. Ultimately, providing cybersecurity through laws and regulations may depend on the current "fear of the day," while the rate of change in computer technology means that even proactive approaches to cybersecurity may lag behind.

6 Conclusion

On the US domestic front, there will continue to be a delicate balancing act between privacy and security. Among the offenses facilitated by the Internet has been the theft of intellectual property, which continues to be a major concern, and it is in this area that law enforcement appears to be most successful in aggressively pursuing offenders under existing laws. Consumer protection legislation requiring stronger reporting requirements when, for instance, banks, credit card companies, and the like have been breached did not fare well in the 112th Congress; nor did legislation designed to protect the nation's critical infrastructure. In terms of the latter, the issue ultimately will revolve around the willingness of the private sector to accept increased regulatory control. The lack of regulatory requirements has been such a critical concern to the executive branch that, after the "watered down" Cybersecurity Act of 2012 was defeated in the Senate, the intense speculation over whether or not the President would issue an Executive Order regulating the nation's critical infrastructure was realized as Congress began its 113th Session and the President his second term in office. Ultimately, the adequacy of US cybersecurity law will continue to be in flux as cyberthreats evolve. As a result, it is imperative that any modifications to existing law be constructed in such a way as to anticipate how the threat landscape may change in the near and distant future.

Acknowledgements: We thank the anonymous reviewers for their comments and suggestions, which greatly helped us to improve the quality and presentation of this paper. We also express our sincere gratitude to the Editor-in-Chief Irmak Renda-Tanali for her strong support and encouragements throughout the preparation of this paper.