**American University Law Review**

Volume 62 | Issue 5 Article 1

2013

# Mapping Today's Cybersecurity Landscape

Jorge L. Contreras
*American University Washington College of Law*

Laura DeNardis
*American University Washington College of Law*

Melanie Teplinsky
*American University Washington College of Law*

# Mapping Today's Cybersecurity Landscape

**Keywords**
America the Virtual: Security, Privacy, and Interoperability in an Interconnected World, United States. Constitution. 3rd Amendment, Cyberspace -- Security measures -- Government policy, Liability (Law) -- United States

# FOREWORD

# MAPPING TODAY'S CYBERSECURITY LANDSCAPE

JORGE L. CONTRERAS*

LAURA DENARDIS**

MELANIE TEPLINSKY***

TABLE OF CONTENTS



* Associate Professor, *American University Washington College of Law.*
** Associate Professor, *American University, School of Communication.*
*** Adjunct Professorial Lecturer, *American University Washington College of Law* and Advisory Board Member, CrowdStrike, Inc.

## I. AMERICA THE VIRTUAL: SECURITY, PRIVACY, AND INTEROPERABILITY IN AN INTERCONNECTED WORLD

Cyberthreats recently overtook terrorism as the number one global threat to America, according to the 2013 global threat assessment performed by the U.S. intelligence community.[1] This special issue of the *American University Law Review* represents the culmination of a concerted effort to bring together scholars, legal practitioners, industry representatives, and government officials to discuss and debate the pressing issues surrounding cybersecurity in today's increasingly interconnected environment. This effort began in October 2012 with a public symposium entitled *America the Virtual: Security, Privacy, and Interoperability in an Interconnected World.* One of the principal themes of the symposium was the growing threat that online security breaches present to business, government, and individual citizens. This *Law Review* issue offers reflections on the symposium, original scholarship, and commentary that we hope will further advance the debate.

### *A. Beyond the Fortress*

Melanie Teplinsky delivered the opening remarks at the symposium in her speech entitled *Beyond the Fortress.*[2] She explained that, for over a decade, the cornerstone of the U.S. approach to cybersecurity has been vulnerability mitigation; that is building stronger fortresses to protect against cyberthreats. While fortification may offer protection against some cyberthreat actors, Teplinsky argued that determined threat actors have the time, resources, and motivation to defeat even the most extensive fortification. Such determined actors may include nation-states, terrorists, and cybercriminals.

Teplinsky described the special challenge that nation-state cyberthreat actors pose to our economic and national security. First, nation-state sponsored cyberespionage poses a serious threat to U.S. economic security. State-sanctioned Chinese hackers are believed to have been stealing not only military secrets, but valuable corporate intellectual property for over a decade, to the detriment of America's

1. *See* Worldwide Threat Assessment of the US Intelligence Community: Hearing Before the S. Select Comm. on Intelligence, 113th Cong. (2013) (statement of James R. Clapper, Director of National Intelligence), *available at* http://intelligence.senate.gov/130312/clapper.pdf.

2. *Welcome Remarks*, AM. U. L. REV., http://aulawreview.org/index.php?view=vidlink&catid=1:symposium-2012&id=154:welcome-remarks&option=com_vidlinks&Itemid=150 (last visited June 15, 2013).

long-term competitiveness.[3] Prominent examples of alleged Chinese cyberoperations include Byzantine Hades,[4] Night Dragon,[5] Operation Aurora,[6] and Operation Shady Rat.[7] Teplinsky also addressed the

3. Michael Riley & Dune Lawrence, *Hackers Linked to China's Army Seen From EU to D.C.*, BLOOMBERG (July 26, 2012, 7:00 PM), http://www.bloomberg.com/news/2012-07-26/china-hackers-hit-eu-point-man-and-d-c-with-byzantine-candor.html (reporting that the stolen information includes seismic maps from oil companies, trade secrets from patent law firms, and market analysis from investment banks).

4. Byzantine Hades refers to a decade-long series of attacks believed to have been perpetrated by the Chinese military. Brian Grow & Mark Hosenball, *Special Report: In Cyberspy vs. Cyberspy, China Has the Edge*, REUTERS (Apr. 14, 2011, 3:52 PM) http://www.reuters.com/article/2011/04/14/us-china-usa-cyberespionage-idUSTRE73D24220110414 (announcing that secret U.S. State Department cables reveal that the Chinese military was involved in "Byzantine Hades, a series of systems breaches, and that "[a]n April 2009 cable even pinpoints the attacks to a specific unit of China's People's Liberation Army"). These attacks are believed to have resulted in the exfiltration of terabytes of sensitive information from the U.S. government and private sector companies, including "designs for multi-billion dollar weapons systems." *Id.*; s*ee also* Jessica Bourquin, The Evolution of Cyber Espionage: A Case for an Offensive U.S. Counterintelligence Strategy 13 (Oct. 14, 2011) (unpublished M.A. thesis, Utica College) *available at* https://www.treadstone71.com/index.php/news-info-whitepapers/masters-in-cybersecurity-intelligence-and-forensics/doc_download/48-the-evolution-of-cyber-espionage-jessica-bourquin; Michael Riley & John Walcott, *China-Based Hacking of 760 Companies Shows Cyber Cold War*, BLOOMBERG (Dec. 14, 2011, 8:47 AM), http://www.bloomberg.com/news/2011-12-13/china-based-hacking-of-760-companies-reflects-undeclared-global-cyber-war.html (noting that the target companies include Google Inc., Intel Corp., and smaller companies like iBahn, a provider of Internet services to hotels); Mathew J. Schwartz, *Leaked Cables Indicate Chinese Military Hackers Attacked U.S.*, INFORMATIONWEEK SEC. (Apr. 19, 2011, 1:09 PM), http://www.informationweek.com/security/attacks/leaked-cables-indicate-chinese-military/229401866 (revealing that Chinese spear-phishing attacks have targeted U.S. government agencies since 2002).

5. Night Dragon is the code name for a cyberespionage campaign leveled against six global oil, energy, and petrochemical companies, including Exxon Mobil, Royal Dutch Shell, and BP. The attack, which is believed to have lasted from 2008–2011, has been described as a "systemic long-term compromise of [the] Western oil and gas industry." DMITRI ALPEROVITCH, MCAFEE, REVEALED: OPERATION SHADY RAT 2 (2011), *available at* http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf. Cyberspies are alleged to have stolen valuable intellectual property, including bidding information; prospecting data, including computerized topographical maps worth "millions of dollars" that show locations of potential oil reserves; and highly sensitive confidential business information. Michael Riley, *Exxon, Shell, BP Said To Have Been Hacked Through Chinese Internet Servers*, BLOOMBERG (Feb. 24, 2011, 3:26 AM), http://www.bloomberg.com/news/2011-02-24/exxon-shell-bp-said-to-have-been-hacked-through-chinese-internet-servers.html The tools, techniques, and network activities associated with the attack were traced back to China. ALPEROVITCH, *supra*, at 2.

6. Operation Aurora refers to a successful cyberespionage campaign against Google and thirty-three other major U.S. companies (reportedly including Intel, Dow Chemical, Morgan Stanley, and computer security guru Symantec). Scott Shane & Andrew W. Lehren, *Leaked Cables Offer Raw Look at U.S. Diplomacy*, N.Y. TIMES (Nov. 28, 2010), http://www.nytimes.com/2010/11/29/world/29cables.html (reporting that leaked American diplomatic cables indicate that "China's Politburo directed the intrusion into Google's computer systems" and that the "Google hacking was part of a coordinated campaign of computer sabotage carried out [in part] by government operatives"). While reports initially suggested that the cyberspies were primarily trying to hack into Gmail accounts of Chinese dissidents as part of an effort to quell dissent,

national security threat posed by nation-state supported cyberattacks on critical infrastructure (CI), such as the August 2012 attack on the world's largest oil company, Saudi Aramco.[8]

Teplinsky concluded that U.S. cybersecurity policy needs to be based not only on vulnerability mitigation, but also on threat deterrence. She emphasized the need to utilize all elements of national power—military, economic, and diplomatic—to deter nation-state actors from engaging in cyberespionage and cyberwar. She also suggested that increased attention to the private sector's role in deterrence may be warranted because the private sector owns the vast majority of CI in the United States,[9] is agile, and has more "eyes on the ground" than the government. In addition, the private sector may be able to help identify actors engaged in cyberespionage and sophisticated cyberattacks and help raise the cost of engaging in such activities.

### *B. The Promise and Peril of Being Interconnected, Interoperable, and Intelligent*

Cybersecurity poses particularly acute challenges for critical components of the national infrastructure. The first symposium panel, entitled *The Promise and Peril of Being Interconnected, Interoperable and Intelligent*,[10] examined cybersecurity implications for standards development within the electric power and healthcare industries. Jorge Contreras, Associate Professor at American University,

---

security experts later opined that the cyberspies were in fact targeting Google's sensitive systems and intellectual property. David Drummond, *A New Approach to China*, GOOGLE OFFICIAL BLOG (Jan. 12, 2010), http://googlepublicpolicy.blogspot.com/2010/01/new-approach-to-china.html.

7. Operation Shady RAT refers to a five-year cyberspying campaign allegedly perpetrated by the Chinese that successfully penetrated the computer networks of more than seventy governments and major corporations, including thirteen defense contractors, in fourteen countries. Approximately fifty of the targets were in the United States. ALPEROVITCH, *supra* note 5, at 3–4; *see* Dean Takahashi, *Black Hat's Spotlight Falls on McAfee's Dmitri Alperovitch for Uncovering Cyber Spying*, VENTUREBEAT (Aug. 4, 2011, 7:00 AM), http://venturebeat.com/2011/08/04/black-hats-spotlight-falls-on-mcafees-dmitri-alperovitch-for-uncovering-cyber-spying (quoting Alperovitch describing Operation "Shady RAT" as the "biggest transfer of wealth in terms of intellectual property in human history").

8. *See* Siobhan Gorman & Julian E. Barnes, *Iran Blamed for Cyberattacks*, WALL ST. J. (Oct. 12, 2012, 7:38 PM), http://online.wsj.com/article/SB10000872396390444657804578052931555576700.html (reporting that the attack used a computer virus to destroy data on 30,000 Saudi Aramco computers).

9. *Critical Infrastructure Sector Partnerships*, DEP'T HOMELAND SEC., http://www.dhs.gov/critical-infrastructure-sector-partnerships (last visited June 15, 2013).

10. *Panel 1: The Promise and Peril of Being Interconnected, Interoperable, and Intelligent*, AM. U. L. REV., http://aulawreview.org/index.php?view=vidlink&catid=1:symposium-2012&id=155:promise-and-peril-of-interconnectivity&option=com_vidlinks&Itemid=150 (last visited June 15, 2013).

Washington College of Law, moderated this panel. Professor Contreras, who teaches and writes about technical standardization, pointed out that 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 today, he observed, is a world that is massively interconnected. Professor Contreras then raised the following question: does interoperability in critical infrastructural assets present additional cybersecurity and privacy challenges, or does it help to prevent and hinder cybersecurity risks?

To set the stage, Tom Kellerman, Vice President of Cybersecurity for TrendMicro,[11] gave preliminary remarks on technological approaches to cyber defense.

Kellerman emphasized that understanding cyber offense informs cyber defense, and he focused on the importance of understanding one's cyberadversaries. 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 (and the associated "bring your own device" phenomenon), 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, Kellerman urged the development of improved standards for browser security, application security, and e-mail authentication.

Following Kellerman's remarks, Dr. George Arnold, National Coordinator for Smart Grid Interoperability at the National Institute of Standards and Technology (NIST), described the massive networking effort currently underway to connect and bring intelligence to the disparate elements of the national power grid. Today's electrical grid, which comprises more than 17,000 power plants, 165,000 miles of high-voltage transmission lines and 3200

11. Kellerman is a former Commissioner for the Commission on Cyber Security for the 44th Presidency, serves on the Board of the National Cyber Security Alliance, and is an adjunct professor at American University's School of International Service.

different electrical utility companies,[12] relies on an infrastructure that has remained largely unchanged for a century. The current Smart Grid effort that NIST coordinates seeks to improve grid efficiency, reliability, and sustainability by using a new generation of smart meters, network sensors, distributed microgrids, and sophisticated monitoring and management systems. With increased interconnection, however, comes increased vulnerability, both to external and internal threats.[13] NIST, other agencies, and the private sector standards-development organizations charged with developing the protocols that will enable Smart Grid interoperability have placed a high priority on securing this key national resource. In addition to security issues, the national Smart Grid will present challenges for maintaining the privacy of data gathered from consumers and households across the country. In an integrated Smart Grid system, information ranging from subscribers' financial and payment data, to energy usage habits, scheduling of daily activities and vacations, and the type and quantity of electrical appliances and devices used, will all become vulnerable to external appropriation and inappropriate use.[14]

Security and privacy issues also play a prominent role in the design of standards for interoperable healthcare systems. Tim Andrews, Vice President of the Booz Allen Hamilton health team, described the potential benefits of moving toward intelligent, interconnected healthcare records systems. These include first order patient care consistency and improvement and second order population-level data analysis for epidemiological and public health applications. With interconnection, however, come heightened risks and vulnerabilities. Health records contain a wealth of personal information about individuals that, if compromised, could give rise to identity theft, financial embezzlement, and healthcare fraud. The medical and healthcare industry is highly fragmented and decentralized, even more than the electrical power grid, involving millions of independent physicians, hospitals, and software vendors.[15]

---

12. George W. Arnold, Remarks at the American University Law Review Symposium: The Promise and Peril of Being Interconnected, Interoperable, and Intelligent: A Smartgrid Perspective (Oct. 25, 2012) (on file with law review).

13. *See, e.g.*, Richard Stone, *A Call to Cyber Arms*, 339 SCIENCE 1026, 1027 (2013) (noting a 2011 report published by Chinese researchers that describes "vulnerabilities in the western U.S. power grid").

14. *See, e.g.*, Ian Brown, *Britain's Smart Meter Programme: A Case Study in Privacy by Design*, INT'L REV. L COMPUTER & TECH. (forthcoming 2013) (manuscript at 2), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2215646.

15. *See* Robert O'Harrow, Jr., *Health-Care Sector Vulnerable to Hackers, Researchers Say*, WASH. POST (Dec. 25, 2012), http://www.washingtonpost.com/investigations/health-

Standardizing and securing a network comprised of disparate and uncoordinated elements will be a tremendous technological and legal challenge.

### *C. Cybersecurity & the Law: Efforts to Address Cybersecurity*

The symposium's second panel focused on recent legal and legislative efforts to address cybersecurity and preserve civil liberties.[16] Lucy Thompson, Chair of the ABA Section of Science & Technology Law, moderated this panel and helped to draw out several themes. First, the panelists emphasized that cybersecurity is a complex problem with many different facets, and that legal and legislative analyses of cybersecurity issues must distinguish not only among different cyberthreat 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 our nation's long-term competitiveness.

Second, the panelists generally agreed with Mike McNerney, former Cyber Policy Advisory in the Office of the Secretary of Defense, and Eric Wenger, Policy Counsel for Microsoft, that the ongoing cybersecurity debate in Congress implicates many longstanding and controversial issues. For example, how do we balance improved cybersecurity that comes in the form of information-sharing or continuous monitoring against the importance of protecting privacy and civil liberties? 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 in ".com" cybersecurity given that the Internet is largely private-sector-owned and operated? Would legislative action, such as setting voluntary cybersecurity standards for critical infrastructure as proposed in the Cybersecurity Act of 2012,[17] incentivize the right behavior or inhibit innovation?

Wenger pointed out that the cybersecurity debate in the 112th Congress reflected a fundamental disagreement over what the

---

care-sector-vulnerable-to-hackers-researchers-say/2012/12/25/72933598-3e50-11e2-ae43-cf491b837f7b_story.html (noting that many medical device manufacturers do not consider cybersecurity risks in manufacturing and medical professionals themselves have already made mistakes leading to breaches).

16. *Panel 2: Cybersecurity & Law*, AM. U. L. REV., http://aulawreview.org/index.php?view=vidlink&catid=1:symposium-2012&id=156:cybersecurity-and-law&option=com_vidlinks&Itemid=150 (last visited June 15, 2013).

17. S. 2105, 112th Cong. (2012).

cybersecurity problem is and which government institution is best situated to address it. Some believe that the most important cybersecurity problem to be solved in the near term 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. The Cyber Intelligence Sharing and Protection Act[18] (CISPA), the narrow information sharing legislation that passed the House in April 2012, is based on this premise. Others 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 Department of Homeland Security take the lead in creating a regulatory model. Both the Senate's Cybersecurity Act of 2012 and its Revised Cybersecurity Act of 2012[19] were based on this premise.

The panelists also discussed the role of the market in cybersecurity. Harriet Pearson, a partner at Hogan Lovells working in the Government Regulatory Practice and Privacy and Information Management Practice and former Chief Privacy Officer for IBM, eloquently argued that we are living in a historic age in which the rapidity of technological change is putting incredible pressure on our business and government institutions. Pearson discussed how technology is fundamentally altering the way in which our organizations work and suggested that law, policy, and market mechanisms are having difficulty keeping pace with these rapid changes. She argued that the market *is* responding to the need for greater security of various types, and that criticisms of the market for not moving fast enough may be overstated given the enormity of the changes the market must accommodate. For example, Pearson argued that industry has made significant changes to address cybercrime and identity theft, and that we are only in the early stages of market response to intellectual property (IP) theft. Finally, she emphasized the need to find policies that will incent the right behaviors without dampening the innovation needed for both good security and a robust economy.

Jessica Herrera-Flanigan, a partner at Monument Policy Group, built on Pearson's remarks, adding that although companies take cybersecurity quite seriously, they are challenged by its increasing complexity, including greater interconnectedness, increased reliance on cloud services, and the trend toward "bring your own device," which

18. H.R. 624 (113th Cong.) (2012).
19. S. 3414, 112th Cong. (2012).

blurs the line between personal and business use of networked devices.

McNerney noted that despite recent SEC guidelines requiring companies to report "material" information regarding cybersecurity risks and cyber incidents,[20] inadequate cybersecurity does not appear to affect the valuation of today's companies; he focused on the need for maturation in insurance and litigation to change this dynamic. McNerney's comments led to a robust discussion regarding the difficulty of assessing both the value of cybersecurity and the costs of cybersecurity failures and the implications of this for the nascent cyberinsurance market.

### *D. Internet Governance: Who Will Lead the Way?*

The third panel of the symposium, entitled *Internet Governance: Who Will Lead the Way?*, addressed the role of Internet governance in shaping the cybersecurity technological, legal, and policy environment.[21] Laura DeNardis, Associate Professor at American University, School of Communication, moderated this panel. She pointed out that Internet governance goes beyond government policies and national law, as technical design also plays a governmental role, corporate policies, and global institutions. The direction of Internet governance, often concealed in technical complexities, is of extreme importance because it will determine the direction of civil liberties online. One theme addressed was the importance of preserving the multistakeholder model of Internet governance that includes the involvement of private industry, civil society, new global Internet governance institutions, and governments.[22] Paul Brigner, Regional Director of the North American Bureau of the Internet Society (ISOC), emphasized that the security and stability of the Internet depend on the preservation of three Internet characteristics: (1) permissionless innovation,[23] (2) open access, and (3) collaboration. Brigner raised concerns about international proposals that might threaten these ideals by imposing a telecommunications model of regulation onto the Internet,

---

20. DIV. OF CORPORATE FIN., SEC, CF DISCLOSURE GUIDANCE: TOPIC NO. 2, CYBERSECURITY (Oct. 13, 2011), http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

21. *Panel 3: Internet Governance: Who Will Lead the Way?*, AM. U. L. REV., http://aulawreview.org/index.php?view=vidlink&catid=1:symposium-2012&id=157:internet-governance-who-leads&option=com_vidlinks&Itemid=150 (last visited June 15, 2013).

22. INTERNET CORP. FOR ASSIGNED NAMES & NUMBERS, ICANN ANNUAL REPORT 2011 (2011) [hereinafter ICCAN REPORT], *available at* http://www.icann.org/en/about/annual-report/annual-report-2011-en.pdf.

23. Permissionless innovation is innovation that can be accomplished without the necessity for obtaining intellectual property permissions or clearances.

affecting issues such as cybersecurity, billing, and quality of service. He also stressed that meetings addressing the future of Internet governance should be open and transparent, providing avenues for multistakeholder dialogue and input. The Internet's role as a shared resource and its architectural blurring of time and space distinctions present unique governance challenges, according to Rashmi Rangnath, Director of the Global Knowledge Initiative at Global Knowledge. Coordination is necessary for the Internet to function, but who has the legitimacy to provide this coordination? Rangnath explained that governance is the act of affecting behavior, ideally reflecting common values. While democracy is the ideal model in the physical world, multistakeholderism is the ideal model in the virtual world. Multistakeholder Internet governance is not a monolithic area, but it involves multiple policy areas such as infrastructure, applications, protocols, and content.[24] As such, Internet governance mechanisms range from tools as diverse as copyright enforcement to net neutrality policies to privacy.

Difficult questions about multistakeholderism, particularly in the area of privacy, include the appropriate role of governments and other specific stakeholders and the appropriate international forums for input from civil society. What should the respective roles of the various stakeholders be? J. Beckwith Burr, Chief Privacy Officer and Deputy General Counsel at Neustar, addressed the question of the role of government in Internet governance and, particularly, how privacy plays out in a virtual world without national borders. One typically thinks about public policy as mediated by governments but this is not always the case in the Internet governance realm. In the view of the Internet Corporation for Assigned Names and Numbers (ICANN), decisions about the operation of country code top-level domains should be managed by the associated country and Internet community.[25] But even in such a case, what if the relevant country passes a law that compromises Internet principles?

Privacy is a similarly complex issue in the multistakeholder world. International trade treaties, for example, usually include privacy rules. But there are significant open debates about privacy, including work in the standards body known as the World Wide Web Consortium (W3C) to create "do not track" mechanisms and work in open international debates about what information should be made

24. *Id.* at 9.
25. *Id.* at 21.

public when you register a domain name.[26] Thomas Smedinghoff, partner at Edwards Wildman Palmer LLP working in the Intellectual Property, Privacy and Data Protection, and Technology, Media and Telecommunications Practice Groups, provided specific examples of online privacy complexities, focusing on governance of specific data transactions in various contexts.

### *E. Keynote: Leap-Ahead Privacy as a Government Responsibility in the Digital Age*

The privacy threats raised by previous speakers were echoed in the keynote address delivered by Ivan Fong, Senior Vice President, Legal Affairs, and General Counsel of 3M Co. and former General Counsel of the U.S. Department of Homeland Security,[27] entitled *Leap-Ahead Privacy as a Government Responsibility in the Digital Age*.[28] Given the many threats incipient in the online environment, Fong identified two primary drivers justifying increased governmental involvement in securing cyberspace: first, the government depends heavily on technology and cyberspace for its own operations; and second, government has a unique vantage point from which to observe and understand global economic, political, and technological forces that could give rise to cyberthreats. He assessed the range of current laws and regulations that address cybersecurity issues, either directly or indirectly, and found them largely inadequate. Thus, Fong recommended that government "leap ahead" with progressive, forward-looking data privacy and security legislation and regulation, rather than waiting for incremental change to occur through judicial intervention.

## II. RECENT DEVELOPMENTS

The world of cybersecurity is fast-moving and several important developments have arisen since the symposium was held in October 2012. First, in February 2013, President Obama issued an Executive Order (EO) on cybersecurity that addressed information sharing as

---

26. *See* Peter Swire, *Full Steam on Do Not Track*, W3C BLOG (Feb. 12, 2013, 11:59 PM), http://www.w3.org/QA/2013/02/full_steam_on_do_not_track.html (reporting that the W3C and a multitude of stakeholders have identified criteria for a successful do not track standard and will now focus on its international aspects).

27. Although Mr. Fong delivered these remarks after his departure from his position as General Counsel of the U.S. Department of Homeland Security in October 2012, they were prepared by Mr. Fong in his official capacity during his tenure with DHS and thus represent views consistent with those of the Administration.

28. Ivan Fong, *Leap-Ahead Privacy as a Government Responsibility in the Digital Age*, 62 AM. U. L. REV. 1131 (2013).

well as the development and implementation of risk-based cybersecurity standards for critical infrastructure.[29] With respect to information sharing, the EO confirmed that it is U.S. policy to improve cybersecurity information sharing by increasing the "volume, timeliness, and quality" of cyberthreat information shared with the U.S. private sector.[30] The EO also put the President's imprimatur on the planned expansion to critical infrastructure companies of an existing information-sharing program between the government and defense industrial base companies.[31] Moreover, under the EO, unclassified versions of reports of cyberthreats to the United States that identify a specific target must be rapidly disseminated to the target.[32] In addition to information sharing, the Order calls for the collaborative development and voluntary adoption of a new cybersecurity framework to include risk-based cybersecurity standards for critical infrastructure.[33]

Second, in March 2013, the U.S. Director of National Intelligence (DNI) identified cyber as the top global threat facing America, stating "it's hard to overemphasize its significance."[34] The next day, President Obama invited select CEOs of CI companies directly to the White House to discuss cybersecurity.[35]

Third, the 2013 National Intelligence Estimate (NIE), a classified document reflecting the "consensus view of the U.S. intelligence community,"[36] reportedly concluded that "the United States is the target of a massive, sustained cyber-espionage campaign that is threatening the country's economic competitiveness."[37] According to press reports, the NIE identifies China "as the country most

29. Exec. Order No. 13,636, 78 Fed. Reg. 11,739 (Feb. 19, 2013).
30. *Id.*
31. *Id.*
32. *Id.*
33. *Id.*
34. *Worldwide Threat Assessment of the U.S. Intelligence Community: Hearing Before the S. Select Comm. on Intelligence*, 113th Cong. 5 (2013) (statement of James R. Clapper, Director of National Intelligence), *available at* http://www.dni.gov/files/documents/Intelligence%20Reports/WWTA%20Remarks%20as%20delivered%2012%20Mar%202013.pdf.
35. Alex Mooney, *President To Host CEOs in Situation Room for Cyber Security Chat*, CNN (Mar. 13, 2013, 1:22 PM), http://security.blogs.cnn.com/2013/03/13/president-to-host-ceos-in-situation-room-for-cyber-security-chat.
36. Ellen Nakashima, *U.S. Said To Be Target of Massive Cyber-Espionage Campaign*, WASH. POST (Feb. 10, 2013), http://articles.washingtonpost.com/2013-02-10/world/37026024_1_cyber-espionage-national-counterintelligence-executive-trade-secrets ("Some officials have pressed for an unclassified summary to be released publicly, [but] . . . as a matter of policy, [the Office of the Director of National Intelligence does] not discuss or acknowledge the existence of NIEs unless directed to do so." (internal quotation marks omitted)).
37. *Id.*

aggressively seeking to penetrate the computer systems of American businesses and institutions."[38] Just days after the NIE was circulated, U.S. information security company Mandiant released a report of over sixty pages offering extensive evidence of Chinese espionage,[39] including actual video of physical intrusion activities.[40]

Fourth, in the area of technical standards and interoperability, the Federal Trade Commission (FTC) has recently demonstrated a strong interest in cybersecurity. In February 2013, the Commission filed a Complaint against HTC America[41] alleging that HTC's smart phones and tablet devices contained various security vulnerabilities, and that the presence of such vulnerabilities constituted unfair and deceptive practices under section 5 of the FTC Act.[42] The action was resolved with the FTC issuing a Consent Order under which HTC agreed to modify specific security vulnerabilities identified by the Commission and to report on security compliance for a period of twenty years.[43] Some commentators have expressed concern that the Commission's action against HTC indicates its willingness to dictate cybersecurity standards absent any regulatory or legislative guidance regarding the scope, nature, or technical details of those standards.[44] Peter Frechette's student Note, FTC v. LabMD*: FTC Jurisdiction Over Information Security is "Plausible," but How Far Can It Go?,*[45] addresses precisely these issues.

Finally, the executive branch has stepped up efforts to deal with cyberespionage through diplomatic channels. In a March 2013 speech to the Asia Society, Tom Donilon, National Security Advisor to the President, unequivocally set forth the expectations of the United States with respect to China's role in cyberespionage, saying:

---

38. *Id.*; *see also* David Barboza, *In Wake of Cyberattacks, China Seeks New Rules*, N.Y. TIMES (Mar. 10, 2013), http://www.nytimes.com/2013/03/11/world/asia/china-calls-for-global-hacking-rules.html ("American intelligence officials have . . . said privately that they have evidence of Chinese government involvement in the [recent hacking] attacks . . . .").

39. MANDIANT, APT1: EXPOSING ONE OF CHINA'S CYBER ESPIONAGE UNITS (2013), *available at* http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

40. *APT1: Exposing One of China's Cyber Espionage Units*, MANDIANT (Feb. 18, 2013), http://www.youtube.com/watch?v=6p7FqSav6Ho.

41. HTC America is the American arm of HTC, a Chinese company that manufactures Android and Windows-based smart phones. HTC, http://www.htc.com/us (last visited June 15, 2013).

42. Complaint, HTC Am., Inc., FTC File No. 122-3049 (Feb. 22, 2013), *available at* http://www.ftc.gov/os/caselist/1223049/130222htccmpt.pdf.

43. *Id.*

44. *See, e.g.*, Allison Grande, *With HTC Deal, FTC Claims Power To Set Security Standards*, LAW360 (Feb. 22, 2013, 8:52 PM), http://www.law360.com/corporate/articles/417857 (discussing the HTC and FTC agreement and the industry reaction to it).

45. Peter Frechette, Note, FTC v. LabMD*: FTC Jurisdiction Over Information Privacy is "Plausible," But How Far Can It Go?*, 62 AM. U. L. REV. 1401 (2013).

> First, we need a recognition of the urgency and scope of this problem and the risk it poses—to international trade, to the reputation of Chinese industry and to our overall relations. Second, Beijing should take serious steps to investigate and put a stop to these activities. Finally, we need China to engage with us in a constructive direct dialogue to establish acceptable norms of behavior in cyberspace.[46]

President Obama himself addressed the issue of nation-state sponsored cyberintrusions in a March 13 interview, stating: "[w]e've made it very clear to China . . . that, you know, we expect them to follow international norms and abide by international rules."[47] When newly elected Chinese President Xi Jinping took office on March 14, 2013, President Obama reportedly called to congratulate Xi and took the opportunity to raise U.S. concerns about hacking.[48] In the course of the call, the two leaders reportedly "committed to engage in an ongoing discussion to address the cyber issue."[49]

The conversation between Obama and Xi appears at a minimum to have accelerated formal diplomatic engagement on cybersecurity between the two countries. On March 17, 2013, just days after the Obama-Xi discussion, the new Chinese Premier Li Keqiang said: "I think we should not make groundless accusations against each other, and spend more time doing practical things that will contribute to cyber-security,"[50] and by mid-April, 2013, U.S. Secretary of State John Kerry announced that the United States and China had agreed to set up a cybersecurity working group.[51]

While the increased diplomatic engagement on cybersecurity is encouraging, substantive progress will take time, and, as the U.S. Under Secretary of State for Economic Affairs has noted: "[i]t's important to have a dialogue on this, but it's also important that the

---

46. Tom Donilon, Nat'l Sec. Advisor to the President, Remarks to the Asia Society: The United States and the Asia-Pacific in 2013 (Mar. 11, 2013), *available at* http://www.whitehouse.gov/the-press-office/2013/03/11/remarks-tom-donilon-national-security-advisory-president-united-states-a.

47. Steve Holland, *Obama, China's Xi Discuss Cybersecurity Dispute in Phone Call*, REUTERS (Mar. 14, 2013, 6:03 PM), http://www.reuters.com/article/2013/03/14/us-usa-china-obama-call-idUSBRE92D11G20130314.

48. *Id.*

49. *Id.*

50. Terrill Yue Jones & Benjamin Kang Lim, *China's New Premier Seeks "New Type" of Ties with U.S.*, REUTERS (Mar. 17, 2013, 4:02 AM), http://www.reuters.com/article/2013/03/17/us-china-parliament-hacking-idUSBRE92G02320130317.

51. Terril Yue Jones, *U.S., China Agree To Work Together on Cyber Security*, REUTERS (Apr. 13, 2013, 11:37 AM), http://www.reuters.com/article/2013/04/13/us-china-us-cyber-idUSBRE93C05T20130413.

dialogue be a means to an end, and the end is really ending these practices."[52]

## III. INSIDE THIS ISSUE

This special issue of the *American University Law Review* supplements and advances the cybersecurity discussion held during its October 2012 symposium with a range of articles and commentary covering different facets of the growing field of cybersecurity. In *Regulating Information Security in the Government Contracting Industry: Will the Rising Tide Lift All the Boats?*, Keir Bancroft observes the increasing trend of federal agencies to mandate information security in their dealings with private contractors. While Bancroft acknowledges the overall societal benefit of reducing cybersecurity risks, he questions the degree to which small organizations lacking the requisite resources, technology, and experience will be able to comply with steadily escalating federal security requirements. In these cases, he argues that emerging businesses may be foreclosed from lucrative government contracts. He then offers several potential solutions that the federal government could implement to assist small businesses in complying with new cybersecurity requirements.

In *When Cyber Weapons End Up on Private Networks: Third Amendment Implications for Cybersecurity Policy*, Alan Butler offers a Third Amendment analysis of military cyberoperations. Butler explores whether, and how, the Third Amendment to the U.S. Constitution—that prohibits quartering soldiers in a house during peacetime without the owner's consent—applies to U.S. military cyberoperations involving government placement of software on privately-owned U.S. networks. Butler makes a novel argument that military software placed on a home or business network constitutes "quartering" of a "soldier" for Third Amendment purposes. He then argues that the Third Amendment confers not merely the narrow right to exclude the military from one's house, but the broader right to exclude the military from one's "private property," including computers and network infrastructure. Building on these arguments, Butler asserts that military cyberoperations could implicate the Third Amendment, and he concludes by exploring ways to design a national cyberoperations strategy informed by Third Amendment principles.

In *Hacker's Delight: Law Firm Risk and Liability in the Cyber Age*, Mike McNerney and Emilian Papadopoulos explore the cybersecurity risks and liabilities that law firms face. McNerney and Papadopoulos begin

52. *Id.*

by exploring who is targeting law firms for cyberintrusion and why; then, he warns that the potential for law firm liability arising out of cyberinstrusions may be increasing. McNerney and Papadopoulos caution that law firms affected by a cyberintrusion could be subject to federal and state data breach notification requirements and SEC disclosure requirements, and that those law firms could face FTC enforcement action for inadequate data security in the event of a data breach. Finally, McNerney and Papadopoulos identify several practical steps that firms can take to protect themselves: implement best practices in cybersecurity risk management, engage senior leadership, encourage a culture of cybersecurity through education and implementation of policies to control cyberrisk, harden networks by implementing effective network security, and formulate crisis response plans.

In his article *Toward Cyber Peace: Managing Cyber Attacks through Polycentric Governance*, Scott Shackelford attempts to shed light on the debate over cybersecurity by conceptualizing cyberspace as a form of "pseudocommons," a "shared global infrastructure" that is regulated by a combination of public and private entities. Shackelford draws on the work of Nobel Laureate Elinor Ostrom, whose groundbreaking work on collective ownership and common resource management revolutionized the field; he finds cyberspace susceptible to vulnerabilities arising from both the well-known "tragedy of the commons" and "anti-commons" paradigms. After considering potential organizational solutions to these problems, he argues that cyber peace is most likely to prevail in an environment of polycentric decision making, modeled, at least in part, on the participatory, bottom-up structure of groups such as the Internet Engineering Task Force (IETF).

In addition to the articles summarized above, this issue includes three student-authored scholarly writings, each of which addresses a discrete, but unsettled, question of cybersecurity law. In the student Comment *Identity Crisis: Seeking a Unified Approach to Plaintiff Standing for Data Security Breaches of Sensitive Personal Information*, Miles Galbraith explores a circuit split on the issue of standing in data breach cases. Galbraith agrees with the holdings of the U.S. Courts of Appeals for the Seventh and Ninth Circuits that an increased risk of identity theft arising out of the theft or loss of personal data constitutes a cognizable injury for purposes of Article III standing, and he rejects the U.S. Court of Appeals for the Third Circuit's view that standing is lacking in the absence of actual misuse of compromised data. Galbraith argues that analogous areas of tort law

support his conclusion that plaintiffs should have standing because theft or loss of personal data constitutes a cognizable injury.

In the first of two student Notes, FTC v. LabMD*: FTC Jurisdiction Over Information Security is "Plausible," But How Far Can It Go?*, Peter Frechette addresses the implications of *FTC v. LabMD* for the FTC's enforcement authority in the data security realm. Section 5 of the FTC Act makes it unlawful to engage in "unfair or deceptive acts or practices in or affecting commerce,"[53] and Frechette explains how *LabMD* may challenge the FTC's authority to regulate unfair data security practices by way of enforcement actions against companies that fail adequately to safeguard sensitive consumer information.

In the second student Note, *Limitations on Employee Liability Under the CFAA After* WEC Carolina Energy Solutions LLC v. Miller, Danielle Sunberg explores an unresolved three-way circuit split over the proper interpretation of the Computer Fraud and Abuse Act provision criminalizing access to a computer "without authorization" or by "exceeding authorized access."[54] At issue is the applicability of this provision to rogue employees who access their company's computer network using valid login information and then steal confidential data from the network in violation of their employer's terms of use. Sunberg explains that the U.S. Circuit Courts of Appeals for the First, Fifth, and Eleventh Circuits—adopting a contract approach—have held that employees "exceed authorized access" when they violate a corporate network's terms of use; the Seventh Circuit—adopting an agency approach—has held that authorization to access the network is terminated when an employee violates his duty of loyalty to his employer; and the U.S. Court of Appeals for the Fourth Circuit—in *WEC*—and the Ninth Circuit—adopting a code-based approach—have held that there is no "unauthorized access" when an employee accesses a company network using the employee's valid login credentials. Sunberg explains that the Fourth Circuit's *WEC* opinion widened the existing circuit split and exacerbated the need for resolution from the Supreme Court or Congress[55] to provide certainty to employers.

---

53. 15 U.S.C. § 45(a)(1) (2006).

54. 18 U.S.C. § 1030(a).

55. Rep. Zoe Lofgren (D–Cal.) has introduced a bill known as "Aaron's Law" to address the circuit split through an amendment to the CFAA, and the House held hearings on the CFAA issue on March 13, 2013. *Investigating and Prosecuting 21st Century Cyber Threats: Hearing Before the Subcomm. on Crime, Terrorism, Homeland Sec. & Investigations of the S. Comm. on the Judiciary*, 113th Cong. (2013). Aaron's Law is named after Aaron Swartz, a brilliant twenty-six-year-old Internet activist who tragically committed suicide in January 2013 while facing prosecution–and potentially thirty-five years of jail time—for violating the above-

## CONCLUSION

Cybersecurity and cyberthreats have risen to prominence in the national public discourse. Private industry, governmental actors, and civil society have recognized these issues as critical to national security, economic competitiveness, and individual rights. We are confident that the timely subjects raised in this issue of the *American University Law Review* represent only the beginning of a debate that is sure to continue for years to come.

---

referenced CFAA provision. Swartz, who fervently believed that information should be made available to the public for free, was being prosecuted for breaking into MIT's computer system and downloading nearly five million articles from a subscription-based academic research database called JSTOR.