EMORY | LAW

Emory Law Journal

Volume 66
Issue 3 *The 2016 Randolph W. Thrower Symposium — Redefined National Security Threats: Tensions and Legal Implications*

Article 3

2017

Cyber Espionage and Electronic Surveillance: Beyond the Media Coverage

William C. Banks

CYBER ESPIONAGE AND ELECTRONIC SURVEILLANCE: BEYOND THE MEDIA COVERAGE

William C. Banks[*]

INTRODUCTION

In the twenty-first century it seems that everyone is eavesdropping on everyone else—governments and companies, militaries, law enforcement and intelligence agencies, hackers, criminals, and terrorists. State-sponsored and private cyber espionage and criminal and foreign-intelligence surveillance have ramped up in part because the national security threat environment is ever more complicated and multifaceted, and the ability to meet it is increasingly dependent on good intelligence, in real time. However, surveillance and espionage have also increased because the Internet and cyber technology so readily enable exploitation of intellectual property and other commercially valuable information. Among its many attributes, the Internet has introduced new dynamics to the age-old tensions between security and liberty. The Internet expands our freedom to communicate at the same time it makes us less secure. It expands our online vulnerabilities while it lowers the visibility of intrusions. The Internet provides new means for enabling privacy intrusions and causing national security and economic harm even as it provides governments with ever more sophisticated tools to keep tabs on bad actors. Yet in the cat and mouse game between the government agents and suspected terrorists and criminals, ever newer devices and encryption programs ratchet up privacy protections in ways that may prevent government access to those devices and their contents. These devices and programs, in turn, may enable cyber theft or even destructive terrorist attacks.

Espionage and intelligence collection are part of the national security apparatus of every state. Cyber espionage involves deliberate activities to penetrate computer systems or networks used by an adversary for obtaining information resident on or transiting through these systems or networks. A pertinent subset is economic espionage, where a state attempts to acquire secrets held by foreign companies. Of course, states conducted economic

[*] Board of Advisers Distinguished Professor, Syracuse University College of Law; Director, Institute for National Security and Counterterrorism.

espionage before the Internet, but the availability of cyber exploitation rapidly and significantly expanded the activity.[1]

Electronic surveillance intercepts communications between two or more parties. The intercepts can give insight into what is said, planned, and anticipated by adversaries. Because such vast quantities of communications now travel through the Internet, more than humans can comprehend in their raw form, surveillance often leads to processing and exploitation through algorithms or other search methods that can query large amounts of collected data in pursuit of more specific intelligence objectives.[2]

Traditional state-sponsored surveillance and espionage have been transformed into high-tech and high-stakes enterprises. Some of the cyber activity is electronic surveillance for foreign intelligence purposes, mimics traditional spying, and services a range of what most of us would concede are legitimate national security objectives—anticipating terrorist attacks, learning about the foreign policy plans of adversaries, and gaining advantage in foreign relations negotiations.[3] However, a good deal of the cyber sleuthing involves economic matters, sometimes extending to include intellectual property theft, and is undertaken by states or their proxies to secure comparative economic advantage in trade negotiations, other deals, or for particular companies.[4]

I. ECONOMIC CYBER ESPIONAGE

Governments and their agents have been exploiting Internet connectivity by penetrating the electronic networks of foreign companies for nearly a quarter-century.[5] Until 2010, companies chose to ignore the problem, more or less.[6] Then Google publicly claimed that China had stolen source code and used it to

---

[1] Gerald O'Hara, *Cyber-Espionage: A Growing Threat to the American Economy*, 19 COMMLAW CONSPECTUS: J. COMM. L. & POL'Y 241, 241–42 (2010).

[2] *See* Joe Pappalardo, *NSA Data Mining: How It Works*, POPULAR MECHANICS (Sept. 11, 2013), http://www.popularmechanics.com/military/a9465/nsa-data-mining-how-it-works-15910146/.

[3] Heather Kelly, *NSA Chief: Snooping Is Crucial to Fighting Terrorism*, CNN (Aug. 1, 2013, 10:35 AM), http://www.cnn.com/2013/07/31/tech/web/nsa-alexander-black-hat/; David E. Sanger, *U.S. Cyberattacks Target ISIS in a New Line of Combat*, N.Y. TIMES (Apr. 24, 2016), http://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html.

[4] *See infra* notes 5–9 and accompanying text.

[5] Joel Brenner, *The New Industrial Espionage*, 10 AM. INT., Winter 2015, at 28, 28–29, http://www.the-american-interest.com/2014/12/10/the-new-industrial-espionage/.

[6] *Id.* at 29.

spy and to penetrate other companies' networks.[7] At about the same time, major economic espionage was carried out against large western oil companies and traced to a site in China, and another theft lifted security key tokens, which in turn led to the penetration of other firms, including defense contractors in the United States.[8]

In May of 2014, the FBI issued "Most Wanted" posters for five Chinese nationals, members of the Peoples' Liberation Army.[9] In *United States v. Wang*, the five were indicted by a federal grand jury for breaking into computer systems of American companies and stealing trade secrets for the benefit of Chinese companies.[10] Although there was no chance that the United States would obtain jurisdiction over the accused so that they could be tried, the indictments may have been intended to incentivize negotiations with the Chinese on corporate spying. At first, the Chinese responded by complaining about U.S. hypocrisy and double standards.[11] The Chinese asserted that American authorities have conducted large-scale, organized cyber-espionage activities against government officials, companies, and individuals, in China and many other states.[12] The distinction that our government draws between spying for national security purposes and not spying on companies to give a competitive edge to one's own businesses is not recognized as valid by China, and they point out that our definition of national security includes obtaining advantages in trade negotiations and for other international economic purposes, including enforcing sanctions regimes and detecting bribery.[13]

Then, in 2015, some seemingly remarkable things happened. Following the indictment of the Chinese hackers and an executive order promulgated by President Barack Obama that authorized sanctions against malicious hackers,[14]

---

[7] Andrew Jacobs & Miguel Helft, *Google, Citing Attack, Threatens to Exit China*, N.Y. TIMES (Jan. 12, 2010), http://www.nytimes.com/2010/01/13/world/asia/13beijing.html.

[8] Nathan Hodge & Adam Entous, *Oil Firms Hit by Hackers from China, Report Says*, WALL ST. J. (Feb. 10, 2011, 12:01 AM), http://www.wsj.com/articles/SB10001424052748703716904576134661111518864; Elinor Mills, *China Linked to New Breaches Tied to RSA*, CNET (June 6, 2011, 4:00 AM), https://www.cnet.com/news/china-linked-to-new-breaches-tied-to-rsa/.

[9] *Cyber's Most Wanted*, FBI, https://www.fbi.gov/wanted/cyber (last visited Apr. 25, 2016).

[10] Indictment, United States v. Wang, Criminal No. 14-118 (W.D. Pa. May 1, 2014), https://www.justice.gov/iso/opa/resources/5122014519132358461949.pdf.

[11] Jonathan Kaiman, *China Reacts Furiously to US Cyber-Espionage Charges*, GUARDIAN (May 20, 2014, 8:31 AM), https://www.theguardian.com/world/2014/may/20/china-reacts-furiously-us-cyber-espionage-charges.

[12] David E. Sanger, *With Spy Charges, U.S. Draws a Line that Few Others Recognize*, N.Y. TIMES (May 19, 2014), http://www.nytimes.com/2014/05/20/us/us-treads-fine-line-in-fighting-chinese-espionage.html.

[13] *Id.*

[14] Exec. Order No. 13,694, 80 Fed. Reg. 18,077 (Apr. 2, 2015).

the United States and China reached an agreement on a range of cybersecurity matters.[15] In addition to cooperation on law enforcement matters in cyberspace, China reversed its prominent policy position and committed not to engage in commercially-motivated cyber espionage.[16] The agreement also includes implementation and compliance provisions, the violation of which could lead to sanctions under the Obama administration executive order.[17]

Although the 2014 indictments had been dismissed as meaningless by many, the Chinese appear not to have understood their lack of practical significance and instead viewed them more like sanctions.[18] The PLA unit also may have felt exposed and diminished in its prestige after the indictments.[19] Meanwhile, news reports indicate that China began to dismantle its economic espionage network and started to crack down on PLA hackers who were moonlighting on the side and selling information to Chinese companies that was not central to the PLA national security mission.[20] A few weeks after the U.S.–China agreement was reached, similar agreements were reached between China and the United Kingdom and China and Germany.[21]

II. SURVEILLANCE

Meanwhile, governments are not the only participants in the cyber-sleuthing. The Islamic State (ISIS) has broadened its recruitment and appeal, focusing in part on young, tech-savvy persons living far from the battlefields of Syria and Iraq.[22] In October 2015, the United States arrested Kosovar Ardit Ferizi while he was living in Malaysia and charged him with providing

---

[15] JOHN W. ROLLINS, CONG. RESEARCH SERV., IN10376, U.S.-CHINA CYBER AGREEMENT (2015), https://www.fas.org/sgp/crs/row/IN10376.pdf.

[16] *Id.*

[17] *Id.*

[18] Ellen Nakashima, *Following U.S. Indictments, China Shifts Commercial Hacking Away from Military to Civilian Agency*, WASH. POST (Nov. 30, 2015), https://www.washingtonpost.com/world/national-security/following-us-indictments-chinese-military-scaled-back-hacks-on-american-industry/2015/11/30/fcdb097a-9450-11e5-b5e4-279b4501e8a6_story.html.

[19] *Id.*

[20] *Id.*

[21] Rowena Mason, *Xi Jinping State Visit: UK and China Sign Cybersecurity Pact*, GUARDIAN (Oct. 21, 2015, 12:13 PM), http://www.theguardian.com/politics/2015/oct/21/uk-china-cybersecurity-pact-xi-jinping-david-cameron; Stefan Nicola, *China Working to Halt Commercial Cyberwar in Deal with Germany*, BLOOMBERG TECH. (Oct. 29, 2015, 8:31 AM), http://www.bloomberg.com/news/articles/2015-10-29/china-working-to-halt-commercial-cyberwar-in-deal-with-germany.

[22] Maeghin Alarid, *Recruitment and Radicalization: The Role of Social Media and New Technology*, *in* IMPUNITY: COUNTERING ILLICIT POWER IN WAR AND TRANSITION 313, 322 (Michelle Hughes & Michael Miklaucic eds., 2016).

material support to terrorism by hacking a U.S. government database and stealing personal information on more than 1350 military and civilian government personnel.[23] Ferizi allegedly passed the information to an operative of ISIS.[24]

The ISIS Cyber Caliphate hacking unit seized control of U.S. Central Command Twitter and YouTube feeds early in 2015, using them to post propaganda videos and personal information on top military officials.[25] The hackers seized more than 54,000 Twitter accounts for the same objectives again late in 2015.[26] Even terrorists who seek visible, kinetic effects from their attacks—and are thus less likely to engage in malware insertion and other disruptive, but not destructive, cyber attacks—increasingly rely on digital protections (encryption) to assure the secrecy of their communications.[27] Most notably, ISIS has demonstrated a sophisticated understanding of methods for shielding its communications from electronic surveillance by intelligence agencies. Security companies have described a manual released by an ISIS operative urging its followers to use fake phone numbers to set up an encrypted chat system that will shield ISIS communications from intelligence surveillance and avoid revealing personal information.[28]

For the most part, international law has been a bystander to this entire fabric of stealth, deception, and greed. The individual strands of this story are bound together by a unique set of oppositional forces and compelling needs for action.

- The costs of economic cyber espionage are staggeringly high and will continue to rise unless something is done.[29]

---

[23] Joe Davidson, *ISIS Threatens Feds, Military After Theft of Personal Data*, WASH. POST (Jan. 31, 2016), https://www.washingtonpost.com/news/federal-eye/wp/2016/01/31/isis-threatens-feds-military-after-theft-of-personal-data/.

[24] *Id.*

[25] CNN Staff, *CENTCOM Twitter Account Hacked, Suspended*, CNN POLITICS (Jan. 12, 2015, 5:43 PM), http://www.cnn.com/2015/01/12/politics/centcom-twitter-hacked-suspended/.

[26] Jigmey Bhutia, *Isis 'Cyber Caliphate' Hacks More than 54,000 Twitter Accounts*, INT'L BUS. TIMES (Nov. 9, 2015, 9:10 AM), http://www.ibtimes.co.uk/isis-cyber-caliphate-hacks-more-54000-twitter-accounts-1527821.

[27] Kate O'Keeffe, *American ISIS Recruits Down, but Encryption Is Helping Terrorists' Online Efforts, Says FBI Director*, WALL ST. J. (May 11, 2016, 8:54 PM), http://www.wsj.com/articles/american-isis-recruits-down-but-encryption-is-helping-terrorists-online-efforts-says-fbi-director-1463007527?mg=id-wsj.

[28] Kim Zetter, *Security Manual Reveals the OPSEC Advice ISIS Gives Recruits*, WIRED (Nov. 19, 2015, 4:45 PM), http://www.wired.com/2015/11/isis-opsec-encryption-manuals-reveal-terrorist-group-security-protocols/.

[29] *See infra* note 53 and accompanying text.

- The Snowden leaks have sewn distrust among citizens and between allied governments, each doubting the veracity of the United States and other nations' intelligence collection practices.[30]
- Intelligence collection incidentally but persistently invades citizens' liberties in collecting beyond the reasonable needs of government.[31]
- Yet continuing terrorist attacks in a wide range of locations reinforces the need for the most effective means of electronic surveillance of potential terrorist activities.[32]
- Traditional espionage is now scapegoated in ways that harm allied relationships and impose costs on intelligence collection.

If we do not act to put a stopper in these escalating crises of costs and confidence soon, the security and integrity of the Internet may be up for grabs. Not to mention the efficacy of intelligence collection by electronic means.

III. THE LIMITED ROLE OF INTERNATIONAL LAW

Cyberspace remains a netherworld for intelligence activities—whatever surveillance or cyber spying a government does outside its own national borders is, in most circumstances, an international law free-for-all. Decades of state practice tell us that surveillance or espionage may be conducted across borders without violating sovereignty.[33] Examples of presumably permissible behavior include collecting the contents of electronic communications or metadata about them; watching government computer systems, including SCADA systems, through cyber penetration; exfiltration of government data, including military or other national security secrets; and denial of service penetrations that decrease the bandwidth for government web sites. Disruptive cyber activities that are not destructive or coercive in some way apparently do not violate international law. The line between permitted espionage and unlawful cyber intrusions is far from clear.

---

[30] Alan Travis, *Snowden Leak: Governments' Hostile Reaction Fuelled Public's Distrust of Spies*, GUARDIAN (June 15, 2015, 11:19 AM), https://www.theguardian.com/world/2015/jun/15/snowden-files-us-uk-government-hostile-reaction-distrust-spies.

[31] *See infra* notes 45–49 and accompanying text.

[32] *See* Kelly, *supra* note 3; Sanger, *supra* note 3.

[33] Glenn Sulmasy & John Yoo, *Counterintuitive: Intelligence Operations and International Law*, 28 MICH. J. INT'L L. 625, 626, 628 (2007).

One response to the increasing concerns about online theft of intellectual property and complaints of invasions of privacy has been for more governments around the world to enact or at least talk about data-localization laws. Such laws, already in place in authoritarian states such as Russia, China, and Iran, typically enforce limitations for all citizen data and the infrastructure that supports it.[34] China strictly vets companies selling Internet technology and services in China.[35] Now-democratic states such as Brazil, India, and Germany are contemplating data-localization. Brazil plans to stop using Microsoft Outlook for e-mail, and Germany has unhooked from Verizon and signed on with Deutsche Telekom.[36] There is talk among our European allies about creating a European Internet.[37]

To what extent does the uniqueness of the cyber domain make cyber espionage and foreign intelligence surveillance legally distinct? On the one hand, the fact that no person has to cross a border to accomplish the espionage or surveillance probably does not matter, legally. Remoteness is just a means of collection. On the other hand, attribution, knowing who stole your secrets, is a serious technical problem and makes controlling cyber exploitation more difficult than keeping tabs on traditional spying. In addition, in the cyber world distinguishing exploitation from a cyber attack (an intrusion designed to disrupt or destroy systems or data) can be difficult. The malware that exploits a computer to retrieve its data may be indistinguishable at first from malware that will destroy the computer hard drive. Thus, the exploited state may be hard-pressed deciding how to prepare and respond.

States have historically tolerated traditional espionage because they all do it and gain from it.[38] Domestic laws proscribe spying for those that are caught. Most espionage disputes are resolved through diplomacy, and in extreme cases, states send the spies home. In cyber espionage, the status quo favors

---

[34] Anupam Chander & Uyên P. Lê, *Data Nationalism*, 64 EMORY L.J. 677, 686–88, 701–02, 735–36 (2015).

[35] Paul Mozur, *New Rules in China Upset Western Tech Companies*, N.Y. TIMES (Jan. 28, 2015), http://www.nytimes.com/2015/01/29/technology/in-china-new-cybersecurity-rules-perturb-western-tech-companies.html?_r=0.

[36] Anton Troianovski & Danny Yadron, *German Government Ends Verizon Contract*, WALL ST. J. (June 26, 2014, 2:54 PM), http://www.wsj.com/articles/german-government-ends-verizon-contract-1403802226; *see also Brazil to Create Its Own Email System After Protesting U.S. Spying*, UPI.COM (Oct. 14, 2013, 5:12 PM), http://www.upi.com/Science_News/Technology/2013/10/14/Brazil-to-create-its-own-email-system-after-protesting-US-spying/69911381785172/.

[37] Sam Ball, *Plans to Stop US Spying with European Internet*, FRANCE 24, http://www.france24.com/en/20140217-european-internet-plans-nsa-spying (last updated Feb. 18, 2014).

[38] *See* Sulmasy & Yoo, *supra* note 33, at 626–29.

sophisticated countries with the finances and technological capabilities to extract the intelligence. But the status quo is changing rapidly. Cyberspace reduces the power differentials among actors. Powerful states have more cyber resources but also more government and private-sector vulnerabilities. The advantage increasingly lies with state-sponsored and non-state hackers—the offense, not the defense—and the costs of cyber exploitation of security and proprietary data are forcing states to look for ways to curb the espionage.

To date, efforts to anchor the law of cyber espionage or foreign-intelligence surveillance in international law have developed in three mostly nascent directions. One potential pathway is the conventional and customary norm of nonintervention, a corollary to state sovereignty. The principle of nonintervention is reflected in Article 2(4) of the U.N. Charter and its prohibition of "the threat or use of force against the territorial integrity or political independence of any state."[39] In theory at least, nonintervention is broader than use of force and the Charter. As the International Court of Justice stated in *Nicaragua v. United States*,[40] wrongful intervention involves "methods of coercion,"[41] and the United States engaged in wrongful intervention even though it did not use force in Nicaragua. Should nonintervention take on new meaning in the twenty-first century based on the expanding cornucopia of technical means for crossing sovereign borders without human intervention? Apart from the technical means, does the contemporary use of state-supported espionage to steal trade secrets and intellectual property constitute intervention? Is a breach of the norm measured by the impact of the intervention, whether virtual or physical? Certainly cyber surveillance or espionage targeting government activities interferes with the internal affairs of the victim state.

However, the legislative history of the Charter and later commentary confirm that "force" in Article 2(4) does not include economic or political pressure.[42] Thus, under the Charter, espionage does not constitute an internationally wrongful act triggering state responsibility under international law. (If a state is responsible for an unlawful act, the victim state is entitled to reparation, and a state may take any responsive actions that neither amount to a

---

[39] U.N. Charter art. 2, ¶ 4.

[40] Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. Rep. 14 (June 27).

[41] *Id.* at ¶ 205.

[42] Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 YALE J. INT'L L. 421, 422 (2011).

use of force nor breach a treaty or customary law obligation. Or it may take countermeasures.)[43] Cyber exploitation directed at financial targets, for example, could cause economic loss, panic in the streets, and a loss of public confidence in the state. Yet if there is no physical damage or loss of life, the Charter suggests that the norm of nonintervention has not been violated.

Some scholars have argued in the alternative that cyber espionage is a lawful precursor to a state's exercise of its U.N. Charter Article 51 self-defense rights.[44] Preparing for and anticipating an armed attack is critically important in the modern world, the argument goes. If not affirmatively allowed as an adjunct to Article 51, others maintain that espionage has been recognized by widespread state practice and thus is supported by a norm of customary international law.

From the human rights perspective, electronic surveillance could be seen to violate the International Covenant on Civil and Political Rights (ICCPR), Article 17(1), which protects against "arbitrary or unlawful interference with . . . privacy."[45] The reach and application of the ICCPR and a similar provision in the European Convention on Human Rights[46] (ECHR) outside any state's territory are unsettled, although there is support for the view that the protection extends to foreign nationals outside the territory of the state party in the context of electronic surveillance or cyber intrusions. The U.N. Special Rapporteur wrote that Article 17 protects against "mass surveillance of the Internet," and that bulk surveillance must be justified following a proportionality analysis that accounts for "systematic interference with the Internet privacy rights of a potentially unlimited number of innocent people located in any part of the world."[47] The Rapporteur finds bulk collection "indiscriminately corrosive of online privacy" and threatening to the core of Article 17 privacy.[48] (Jurisdictional issues cloud whether any court or treaty body would apply human rights law to surveillance or cyber spying.) Cases are

---

[43] Michael N. Schmitt, *"Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law*, 54 VA. J. INT'L L. 697, 703 (2014).

[44] Ashley Deeks, *An International Legal Framework for Surveillance*, 55 VA. J. INT'L L. 291, 302 (2015); *see also* U.N. Charter art. 51 ("Nothing in the present Charter shall impair the inherent right of individual or collective self-defense . . . .").

[45] International Covenant on Civil and Political Rights art. 17, ¶ 1, Dec. 19, 1966, 999 U.N.T.S. 171.

[46] Convention for the Protection of Human Rights and Fundamental Freedoms art. 8, Nov. 4, 1950, 213 U.N.T.S. 221.

[47] U.N. Secretary-General, *Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism*, ¶ 59, U.N. Doc. A/69/397 (Sept. 23, 2014).

[48] *Id.*

pending now in the European Court of Human Rights alleging privacy violations due to the U.K. Government Communications Headquarters's cooperation with the National Security Agency in collecting upstream contents and bulk data.[49]

An unusual alignment of interests between some powerful governments (victims of cyber exploitation and overbroad surveillance), ordinary citizens, and major corporations and their clients present what may be a propitious time for forging new international law in these areas. Governments, citizens, and influential opinion makers learned a great deal about foreign intelligence surveillance from the Snowden leaks. And the governments most affected by the Snowden leaks are some of the same ones most victimized by cyber espionage of one sort or another.

The United States has already begun to limit their surveillance activities in response to political pressure, not least from the heads of state whose conversations were recorded.[50] Meanwhile, litigation in European and U.S. courts and a resolution by the U.N. General Assembly addressing the right of privacy in the digital era[51] sow the seeds of a rights-based reorientation of international law. Perhaps most important, the economic impacts of cyber espionage and foreign surveillance are considerable. On the surveillance side of things, Internet service providers and social media companies in the United States are losing contracts and clients in many places, and the data-localization laws and other steps taken by some states to insulate "their" piece of the Internet threaten to further constrain the global economy.[52] As for cyber

---

[49] *See, e.g.*, Applicant's Reply, 10 Human Rights Orgs. v. United Kingdom, App. No. 24960/15 (2016), https://www.documentcloud.org/documents/3115985-APPLICANTS-REPLY-to-GOVT-OBSERVATIONS-PDF.html; Ryan Gallagher, *Europe's Top Human Rights Court Will Consider Legality of Surveillance Exposed by Edward Snowden*, INTERCEPT (Oct. 3, 2016), https://theintercept.com/2016/09/30/echr-nsa-gchq-snowden-surveillance-privacy/.

[50] Presidential Policy Directive PPD-28: Directive on Signals Intelligence Activities, 2014 DAILY COMP. PRES. DOC. 31 (Jan. 17, 2014); REVIEW GROUP ON INTELLIGENCE AND COMMC'NS TECHS., LIBERTY AND SECURITY IN A CHANGING WORLD: REPORT AND RECOMMENDATIONS OF THE PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES 20 (2013), https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf (suggesting steps to place certain allied leaders' private communications off-limits for the NSA).

[51] Human Rights Council, Rep. of the Office of the U.N. High Comm'r for Human Rights, The Right to Privacy in the Digital Age, U.N. Doc. A/HRC/27/37 (June 30, 2014).

[52] Claire Cain Miller, *Revelations of N.S.A. Spying Cost U.S. Tech Companies*, N.Y. TIMES, (Mar. 21, 2014), http://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html.

espionage, the estimated $300–600 billion annual price tag[53] is illustrative of the costs imposed by theft of IP and trade secrets, along with other valuable government and private sector information.

States could agree to distinguish national-security espionage from all other forms, and tolerate only the former. After all, keeping a nation safe is a high and noble objective, and intelligence can directly serve that end. The trick is to thoughtfully limit that power to collect intelligence only where it is necessary to safeguard national-security interests, and then to be sure that the intelligence function is subject to effective oversight. All other forms of espionage could be treated as theft, and rules forbidding that activity could be enforced in the private, commercial realm. It remains difficult in some instances to distinguish national-security espionage from other spying. Developing customary international law is a slow, lengthy process, but it could begin in just this way. If a sufficient number of other states sign on, new international norms may be made. A similar process could lead to developing international law on surveillance, perhaps starting with agreements among the Five Eyes—the English speaking democracies.

Similarly, states could agree that international law forbids spying by a state for the direct benefit of a private company. Governments can and have at times established rules of the road for limiting espionage and created incentives for cooperation. The 2015 U.S.–China agreement is exemplary.[54] The new approaches are necessary because the model response to conventional espionage—arrest their spies, expel diplomats, and the like—does not work when the cyber theft is accomplished remotely by unnamed agents. Trade sanctions, tariffs, and diplomatic pressures are often effective tools.

Another method of influencing international law could be to adapt domestic laws to international law. Domestic regulation of cyber espionage in the United States has been provided by the Economic Espionage Act (EEA), which proscribes the possession, collection, duplication, transfer, or sale of trade secrets for the benefit of a foreign nation or any of its agents.[55] The Justice Department is expressly given extraterritorial enforcement authority.[56]

---

[53] Ellen Nakashima & Andrea Peterson, *Report: Cybercrime and Espionage Costs $445 Billion Annually*, WASH. POST (June 9, 2014), https://www.washingtonpost.com/world/national-security/report-cybercrime-and-espionage-costs-445-billion-annually/2014/06/08/8995291c-ecce-11e3-9f5c-9075d5508f0a_story.html (CSIS places the figure at $375–$575 billion).

[54] *See supra* notes 15–21 and accompanying text.

[55] 18 U.S.C. § 1831 (2012).

[56] 18 U.S.C. § 1836 (2012).

Amendments to the EEA in 2012 and 2013 increased the criminal penalties and the breadth of coverage for stealing trade secrets to benefit a foreign government.[57] New amendments have been recommended that would provide a private right of action for those who hold trade secrets that have been subject to theft.[58] In addition, the Computer Fraud and Abuse Act (CFAA) prohibits intentionally causing damage through a computer code or program to any computer connected to the Internet.[59] Although not written with espionage in mind, the CFAA could be used to counter cyber exploitation. These domestic laws could provide foundational concepts for developing international agreements and, eventually, international law.

The benefits of augmenting international law with domestically grown mechanisms are numerous, but ultimately, customary international law needs an international platform. For example, in the intellectual property realm, customary international law could incorporate intellectual property theft proscriptions from the World Trade Organization (WTO) and the related Trade Related Aspects of Intellectual Property Rights agreement.[60] An advantage is the use of a respected international forum, where nations such as China could also seek relief from cyber exploitation (by the United States). A drawback is that WTO agreements presently require meeting obligations only within the member's territory.[61] The structure of the agreements could be changed, if they could figure out how to prove responsibility for a state's actions outside its territory.

In an effort to distinguish espionage while applying domestic legal structures, states could determine that disruptive cyber actions should be treated differently than espionage. Such agreements could be grafted onto the Cybercrime Convention.[62] The Cybercrime Convention commits states to enact domestic laws criminalizing cyber theft.[63] Of course, the Cybercrime Convention could be amended to make unlawful espionage that steals trade secrets or other proprietary information for the benefit of domestic firms. The domestic laws required by the Convention are largely ineffective against state-

---

57 *Id.*

58 Dennis Crouch, *Defend Trade Secret Act Moving Forward*, PATENTLY-O (Apr. 5, 2016), http://patentlyo.com/patent/2016/04/secret-moving-forward.html.

59 18 U.S.C. § 1030 (2012).

60 Agreement on Trade-Related Aspects of Intellectual Property Rights, Apr. 15, 1994, 1869 U.N.T.S. 299.

61 *See, e.g.*, *id.* art. 1, ¶ 1.

62 Convention on Cybercrime, Nov. 23, 2001, 2296 U.N.T.S. 167.

63 *Id.* art. 2.

sponsored theft because of the difficulties of obtaining jurisdiction of accused cyber criminals and because of diplomatic immunities. The domestic laws are difficult to enforce anyway because of attribution problems. There are no enforceable international law violations recognized by the treaty. As it now stands, the Cybercrime Convention includes no universal definition of cybercrime, for example.[64] Does cybercrime include theft for espionage purposes? The Convention has demonstrated that problems of cyber espionage cannot be addressed as a traditional crime problem because a large portion of what is criminal is state-tolerated or state-supported. Nor are Mutual Legal Assistance Treaties useful where the crimes are politically motivated and state sponsored.

Furthermore, distinguishing between cyber espionage and disruptive cyber activity could encourage states to come to agreements upon some off-limits parts of cyber. For example, agreements not to disrupt nuclear installations or other critical infrastructure would be beneficial to all sides. Abolishing spying on these systems goes hand in hand with limiting disruption. Once the infrastructure is off-limits for attack, there is no legitimate reason to illicitly obtain information about that system.

CONCLUSIONS

The confluence of interests between victims of overbroad surveillance and cyber espionage presents an opportunity to begin developing new norms and eventual international law that could bring more rationality, predictability, and privacy protections to the cyber domain. The costs of cyber espionage are real, and the threats and vulnerabilities will increase with the progression of technology. Companies and governments are underprepared for the level of cyber espionage they are facing. Solutions vary, but they all share the common foundation of increased international cooperation and the development of a customary international legal framework that everyone understands.

Meanwhile, blowback from the Snowden leaks has generated sufficient political pressure to cause some changes to surveillance authorities. As those reforms develop and privacy claims are litigated in international fora and European courts, it is likely that new international law will emerge, too, perhaps in tandem with reforms to the limits on cyber espionage.

---

[64] *Id.* art. 1.