5-1-2016

# A Comparative Approach to Economic Espionage: Is Any Nation Effectively Dealing With This Global Threat?

Melanie Reid

# A Comparative Approach to Economic Espionage: Is Any Nation Effectively Dealing With This Global Threat?

MELANIE REID*

*In 1996, Congress passed the Economic Espionage Act (EEA), 18 U.S.C. Sections 1831 and 1832, to help thwart attempts by foreign entities intent on stealing U.S. proprietary information and trade secrets. Despite the passage of the EEA almost twenty years ago, if recent statistics are to be believed, there is so much trade secret thievery going around that the United States finds itself in the midst of an epidemic of economic espionage. Currently, any and all U.S. technology that is vulnerable and profitable is being targeted. Unfortunately, existing remedies and enforcement have barely blunted the onslaught against the U.S. which faces, according to the IP Commission Report, a potential 300 billion dollar loss of raw innovation every year. To date, there have only been a handful of § 1831 convictions since the Act was passed. That is hardly a deterrence or something to send shudders down the backs of would-be industrial spies. Despite U.S. shortcomings, the rest of the world has not done any better.*

* Associate Professor of Law, Lincoln Memorial University-Duncan School of Law. I would like to thank Bethany Thompson and Gordon Russell for their invaluable research assistance, Andrea Dennis, Shawn Boyne, Timothy Webster, Akram Faizer, Bruce Beverly, and Syd Beckman for their excellent editorial comments, and Pat Laflin who is an expert in this field. Additional thanks goes to all the SEALS 2015 Conference participants who provided me with significant comments and advice during my presentation of this paper.

*This article explores the reasons behind the U.S. government's two-pronged approach: preventing the thefts by educating and training private companies to improve security and safeguard their secrets, and reacting to acts of economic espionage by federally prosecuting offenders under the EEA, and why this approach is not succeeding. The U.S. approach has been weak for several reasons: (1) the EEA, specifically, 18 U.S.C. § 1831, has been difficult to prove; (2) the sentences under § 1831 have been minimal; (3) despite being educated on the pitfalls of lax cybersecurity and personnel controls, there is a lack of buy-in from private industry to cooperate with law enforcement and/or tighten office security measures to prevent IP theft; (4) the federal government has taken a relatively hands-off approach in assisting private enterprise; and (5) other countries do not assist in international investigations due to their own weak response or individual attitudes towards intellectual property theft or in some cases, are the same foreign countries involved in the theft. This article also examines how various countries are handling the economic espionage threat and how differences in cultural, historical, and nationalistic backgrounds as well as economic and political governance allow some countries to be unapologetic supporters of state-sponsored economic espionage. The overall global response to economic espionage is weak, and a stronger U.S. response is needed.*

## I. INTRODUCTION

"Our workers are the most productive on Earth, and if the playing field is level, I promise you—America will always win." – Pres. Barack Obama[1]

When Americans are asked the question, what is the single, greatest foreign threat to our nation's economic health and stability, many will say it is the transfer of American manufacturing jobs to other countries such as China and Korea. While it is true that millions of manufacturing jobs have been moved overseas,[2] there is an

---

[1] EXEC. OFFICE OF THE PRESIDENT OF THE UNITED STATES, ADMINISTRATION STRATEGY OF MITIGATING THE THEFT OF U.S. TRADE SECRETS 7 (2013), https://www.whitehouse.gov/sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf [hereinafter TRADE SECRETS].

[2] PETER NAVARRO & GREG AUTRY, DEATH BY CHINA: CONFRONTING THE DRAGON—A GLOBAL CALL TO ACTION (Prentice Hall 2011). "Since China joined the World Trade Organization in 2001 and falsely promised to end its mercantilist and protectionist practices, America's apparel, textile, and wood furniture industries have shrunk to half their size—with textile jobs alone beaten down by 70%.

even greater threat to our nation's economic productivity and prosperity: economic espionage.

Economic espionage occurs when a foreign power sponsors or coordinates intelligence activity directed at another government, a foreign corporation, establishment, or person.[3] This intelligence activity is "designed to unlawfully or clandestinely . . . obtain sensitive financial, trade, or economic policy information; proprietary economic information; or critical technologies[,] or to unlawfully or clandestinely influence sensitive economic policy decisions."[4] An employee's unwitting act of opening an electronic attachment containing a malicious virus meant to infiltrate the company's server or a trusted insider who deliberately downloads his employer's source code for personal gain and for the benefit of a foreign entity can harm the employer and may cost their company millions or even billions of dollars.[5]

The term "economic espionage" sounds mysterious and perhaps a bit "cloak and dagger." One can imagine a covert foreign agent tasked with committing economic espionage stopping by a dead drop to retrieve a package containing the latest blueprints or prototype designs that a General Electric employee has left behind for his handler. However, one who commits economic espionage needs no covert moves to be successful.

In reality, economic espionage is merely a form of cheating—stealing trade secrets from one company in order to assist a state-

---

Other critical industries like chemicals, paper, steel, and tires are under similar siege, while employment in our high-tech computer and electronics manufacturing industries has plummeted by more than 40%." *Id.* at 2–3.

[3] DEP'T OF JUSTICE, FED. BUREAU OF INVESTIGATION, ECON. ESPIONAGE, PROTECTING AMERICA'S TRADE SECRETS, https://www.fbi.gov/about-us/investigate/counterintelligence/economic-espionage-1. Industrial espionage is similar to economic espionage in that it involves the theft of trade secrets, however, industrial espionage does not involve a foreign power, instrumentality, or agent. *Id.* at 2.

[4] The FBI Fed. Bureau of Investigation, *Frequently Asked Questions* (last visited Oct. 22, 2015) https://www.fbi.gov/about-us/faqs.

[5] "Cyber espionage is the science of covertly capturing e-mail traffic, text messages, other electronic communications, and corporate data for the purpose of gathering national-security or commercial intelligence." Seymour M. Hersh, *The Online Threat: Should we be worried about a cyber war?*, THE NEW YORKER, Nov. 1, 2010, http://www.newyorker.com/magazine/2010/11/01/the-online-threat.

sponsored foreign entity skip its research and development (R&D) phase (or at least, accelerate the process) and proceed straight to making money for its stakeholders and boost that country's economy. What makes this form of cheating "espionage" is that typically, one foreign nation is deprived of its trade secrets while another benefits from its neighbor's sweat equity.

In 1996, the United States' Congress determined that this is a crime.[6] Some nations agree, others condemn the activity but let the civil courts handle these issues, and other nations condone it—all is fair in love, war, and business.[7] One nation's political and military ally can also be that country's economic competitor/adversary at the same time.

While the threat may sound exaggerated, it is not. Estimates vary, but economic espionage costs the United States' government and the private sector somewhere between $2 to $400 billion annually.[8] Symantec, an American technology security company, estimates that industrial espionage costs United States' businesses more than $250 billion each year.[9] Others have calculated that cyber espionage, in particular, costs the U.S. economy from 0.1 percent to 0.5 percent of its gross domestic product.[10]

---

[6] Economic Espionage Act of 1996, Pub. L. No. 104–294, 110 Stat. 3488.

[7] Siobhan Gorman, *China Singled Out for Cyberspying*, THE WALL STREET JOURNAL (Nov. 4, 2011), http://www.wsj.com/articles/SB10001424052970203716204577015540198801540.

[8] The U.S. International Trade Commission estimated in 2009 that as much as $50 billion was lost due to espionage, cyber attacks and other counterfeit and trademark crimes. OFFICE OF THE NATIONAL COUNTERINTELLIGENCE EXEC., FOREIGN SPIES STEALING U.S. ECONOMIC SECRETS IN CYBERSPACE: REPORT TO CONGRESS ON FOREIGN ECONOMIC COLLECTION AND INDUSTRIAL ESPIONAGE 2009-2011 (2011) [hereinafter COUNTERINTELLIGENCE REPORT]. *See also* David Cotriss, *Blame Game: Cyber Espionage*, SC MAGAZINE (Nov. 1, 2013), http://www.scmagazine.com//blame-game-cyber-espionage/printarticle/316384/.

[9] Cotriss, *supra* note 8. *See also* MCAFEE CENTER FOR STRATEGIC AND INT'L STUDIES, NET LOSSES: ESTIMATING THE GLOBAL COST OF CYBERCRIME (2014), http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf.

[10] Ellen Nakashima, *Obama Orders Voluntary Security Standards for Critical Industries' Computer Networks*, THE WASHINGTON POST (Feb. 12, 2013), https://www.washingtonpost.com/world/national-security/obama-orders-voluntary-security-standards-for-critical-industries-computer-networks/2013/02/12/e1d0a586-755e-11e2-8f84-3e4b513b1a13_story.html.

During a Senate hearing in 2014, Representative Mike Rogers, chair of the House Intelligence Committee and chairman of the Permanent Select Committee on Intelligence, stated that the theft of proprietary information and technology constitutes "the largest transfer of wealth . . . in the world's history"[11] and has cost the

---

The Commission on the Theft of American Intellectual Property reports that annual U.S. economic losses from international IP theft are "likely to be comparable to the current annual level of U.S. exports to Asia, [which is estimated at] over $300 billion." COMM'N ON THE THEFT OF AM. INTELL. PROP., THE IP COMMISSION REPORT 2 (2013). "[F]ormed in 2012, [the Commission on the Theft of American Intellectual Property is] 'an independent initiative representing the sectors of research, defense, academia, government, labor, and business. The Commission is dedicated to examining the causes and impact of IP theft on U.S. strategic and economic interests and recommending policy solutions to the Administration and Congress.'" Scott Bradner, *IP Commission Report: Surprisingly Clueful*, NETWORK WORLD (May 30, 2013), http://www.networkworld.com/article/2166743/software/ip-commission-report--surprisingly-clueful.html. A threat assessment statement from 2015 outlining the top risks to national security found that dangers from foreign spies and from leakers "are increasing in frequency, scale, sophistication, and severity of impact." *Worldwide Threat Assessment of the U.S. Intelligence Community: Hearing Before Senate Armed Services Comm.*, 114th Cong. 1–3 (2015) (statement for the record of James R. Clapper, Director of National Intelligence), http://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf. According to Clapper's statement, the top threats in 2014 included: 1) cyberattacks, cyberespionage, 2) terrorism and transnational organized crime, 3) Weapons of Mass Destruction proliferation, 4) counterintelligence, and 5) counterspace (attacks on satellites, communications). *Id.*

[11] Hilary Tuttle, *Counterintelligence Now Riskier than Terrorism, Intelligence Officials Report*, RISK MANAGEMENT MONITOR (Jan. 30, 2014), http://www.riskmanagementmonitor.com/counterintelligence-now-riskier-than-terrorism-intelligence-officials-report/. An economist and director of the U.S. Cyber Consequences Unit, a non-profit research institute, has said, "While a precise dollar figure for damage is elusive, the overall magnitude of the attacks is not. We're talking about stealing entire industries. This may be the biggest transfer of wealth in a short period of time that the world has ever seen." Michael Riley & John Walcott, *China-Based Hacking of 760 Companies Shows Cyber Cold War*, BLOOMBERG BUSINESS (Dec. 14, 2011), http://www.bloomberg.com/news/articles/2011-12-13/china-based-hacking-of-760-companies-reflects-undeclared-global-cyber-war. This is a common phrase used by those describing the impact of economic espionage. The cybersecurity "firm McAfee detailed hacks into some 72 public and private computer networks in 14 countries [in a report in August 2011] and [also] warned of 'the biggest transfer of wealth in terms of intellectual property in history.'" Adam Piore, *Digital Spies: The Alarming Rise of Electronic Espionage*, POPULAR MECHANICS (Jan. 24, 2012),

United States an estimated $2 trillion.[12] One thing is certain, the United States would stand to gain millions of jobs and see a dramatic increase in GDP growth, R&D investment, and increased worker productivity and innovation in a world where economic espionage disappeared and a respect for intellectual property existed. Pens, papers, files, and document storage rooms are a thing of the past. We currently live in an age of malware[13], botnets[14], rootkits,[15] zero-

---

http://www.popularmechanics.com/technology/security/how-to/a7488/digital-spies-the-alarming-rise-of-electronic-espionage/.

[12] *See* Tuttle, *supra* note 11. *See also Ann. Open Hearing on Current and Projected National Security Threats to the U. S.: Hearing Before Senate Select Comm. on Intelligence,* 113th Cong. 4–7, 12–14 (2014) [hereinafter *Senate Hearing*] (statement of James R. Clapper, Director of National Intelligence). This threat assessment report outlines the top risks to national security. The report says dangers from foreign spies and leakers have increased in frequency and severity.

[13] Malware can be embedded on microchips purchased by a company and used to exfiltrate information from computers. *Hearing Before the Subcomm. on Crime and Terrorism of the Senate Comm. on the Judiciary*, 112th Cong. 6–8 (2011) (statement of Gordon Snow, Assistant Dir., Cyber Div., Fed. Bureau of Investigation).

[14] DEP'T OF DEFENSE, DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE (Jul. 2011). "Botnets are networks of compromised computers controlled remotely by an attacker. The botnets run by criminals could be used by cyber terrorists or nation states to steal sensitive data, raise funds, limit attribution of cyber attacks, or disrupt access to critical national infrastructure. Botnets that specialize in data exfiltration are able to capture the contents of encrypted webpages and modify them in real time. When properly configured, criminals can ask additional questions at login or modify the data displayed on the screen to conceal ongoing criminal activity." Snow, *supra* note 13.

[15] Thomas Brewster, *Russians Suspected in 'Uroburos' Digital Espionage Attacks*, TECH WEEK EUROPE (Mar. 3, 2014, 11:24 AM), http://www.techweekeurope.co.uk/workspace/russian-intelligence-uroburos-malware-140494 (quoting Jaime Blasco, director of AlienVault Labs). A "root kit" is a type of malware that "hides the presence of the spying operation and also creates a hidden, encrypted file system to store stolen data and tools used by the attackers. Those tools include password stealers, tiny programs for gathering information about the system and document stealers." *Id*; Peter Apps & Jim Finkle, *Insight – Suspected Russian Spyware Turla Targets Europe, U.S.*, REUTERS (Mar. 7, 2014, 2:31 PM), uk.reuters.com/article/2014/03/07/russia-cyberespionage-idUKL1N0M302H20140307.

day,[16] honeypots,[17] cybercriminal threats, advanced persistent threats (APTs)[18] and computer network exploitation. It is relatively easy for nation states to either steal trade secrets via the internet or to find an insider who will steal it for them. These significant and repeated threats should raise our ire and cause entrepreneurs to take a second look at their electronic encryption process or personnel security measures. Yet surprisingly, most Americans remain either indifferent to this present and persistent threat, lulled into a false sense of security due to the inadequate protective measures already in place, or resigned to the possibility of technology loss through theft as just another cost of doing business. Their concerns only become truly real when it becomes personal, when it is their company trade secrets that are looted.

Foreign competitors steal trade secrets in a variety of ways—through targeting and recruiting insiders, conducting economic intelligence operations through the use of bribery, cyber intrusions, theft, and dumpster diving in search of intellectual property or discarded prototypes, and establishing joint ventures with U.S. companies.[19] Foreign competitors will also utilize unsolicited emails to tar-

---

[16] Zero-day refers to a Windows software flaw that was used by Russian government-linked hackers to install malicious software to conduct a large-scale cyber-spying program on NATO, U.S. government agencies, and European countries. Ellen Nakashima, *Hackers Breach Some White House Computers*, THE WASHINGTON POST (Oct. 28, 2014), www.washingtonpost.com/world/national-security/hackers-breach-some-white-house-computers/2014/10/28/2ddf2fa0-5ef7-11e4-91f7-5d89b5e8c251_story.html.

[17] Economic Espionage professionals defined "Honeypots" as "intelligence operations in which a younger sexual partner is used to seduce and suborn a target with access to secret information." Susan Waterman, *U.S. Defense Contractor Arrested for Passing Secrets to Chinese 'Honeypot,'* WASHINGTON TIMES (March 19, 2013) http://www.washingtontimes.com/news/2013/mar/19/us-defense-contractor-arrested-passing-secrets-chi/?paige=all.

[18] An "advanced persistent threat" is considered "an onslaught of computer network intrusions originating from Internet Protocol (IP) addresses in China." COUNTERINTELLIGENCE REPORT, *supra* note 8, at 5. The Department of Defense has characterized China as "the world's most active and persistent perpetrator of economic espionage." Cotriss, *supra* note 8.

[19] *Economic Espionage And Trade Secret Theft: Are Our Laws Adequate For Today's Threats? Hearing Before Senate Comm. on the Judiciary, Subcomm. on Crime and Terrorism*, 113th Cong. (2014) [hereinafter Coleman Statement]

get insiders or plant a computer virus, establish front companies, liaison with universities that have ties to defense contractors, have foreign intelligence agents attempt to recruit insiders, serve as hosts or attendees at trade conferences, infiltrate research and facilities relocated overseas, circumvent export control laws, visit scientific and research delegations, and of course, hack into private company databases.[20]

The United States government recognizes that economic espionage is a huge problem, so it has taken steps to combat and protect against this threat. But are these protective measures sufficient to thwart or mitigate the problem? Should the United States reverse course and follow the path of other nations, which steal foreign intellectual property and share the pilfered trade secrets with their own state-run industries and corporations? Or should we simply look the other way like other countries appear to be doing? This article examines how various countries deal with the economic espionage threat and how these measures compare to the U.S. response; it seeks to explore how differences in national pride, cultural, historical and nationalistic backgrounds, and economic and political governance allow some countries to be unapologetic supporters of state-sponsored economic espionage. Part II evaluates the U.S. government response and how other countries handle the issue of economic espionage, which countries have chosen to criminalize these acts and which countries condemn but do not criminalize. Part III identifies the leading offender nations and how cultural attitudes toward property rights and the type of political governance contribute to an acceptance of economic espionage. Part IV attempts to explain why the overall global response to economic espionage is weak, why the issue is more complicated than it seems at first glance, and why a strong U.S. response is needed.

---

(statement of Randall C. Coleman, Assistant Dir. Counterintelligence Div., Fed. Bureau of Investigation).

[20] FBI NATIONAL PRESS OFFICE, FBI ANNOUNCES ECONOMIC ESPIONAGE AWARENESS CAMPAIGN (2015); Coleman Statement, *supra* note 19.

## II. GLOBAL SOLUTIONS TO COMBAT ECONOMIC ESPIONAGE

### A. *The United States' Response*

The U.S. government is currently using a two-pronged approach to combat economic espionage by: (1) preventing the thefts by educating and training private companies to improve security and safeguard their secrets, and (2) reacting to acts of economic espionage by federally prosecuting offenders.[21]

The Federal Bureau of Investigation (FBI) is the leading agency responsible for combatting economic espionage. In fact, counterespionage[22] has become their number two priority second only to terrorism.[23] Intellectual property theft not only costs businesses money, but it is also considered a strategic threat—a threat to our nation's economic and security interests.[24]

---

[21] *See generally* COVINGTON & BURLING LLP, ECONOMIC ESPIONAGE AND TRADE SECRET THEFT: AN OVERVIEW OF THE LEGAL LANDSCAPE AND POLICY RESPONSES (2013).

[22] Counterespionage includes corporate counterintelligence, which is considered the reverse form of business espionage and business intelligence. Its main purpose is to protect business information from those who are not authorized to receive it, to counter potential threats, and to enhance security. *See* Steve Whitehead, *Corporate Counterintelligence—Protecting Business Information*, COMPUTER BUS. REV. (June 1, 2013), http://www.cbr.co.za/regular.aspx?pklRegularId=1390.

[23] "F.B.I. Director Robert Mueller designated espionage as the F.B.I.'s number two priority." *Investigative Programs Counterintelligence Division*, The Federal Bureau of Investigation (Last visited Nov. 3, 2015), https://www2.fbi.gov/hq/ci/economic.htm. *See also A New F.B.I. Focus: H.R. Comm. on Appropriations, Subcomm. for the Dep't of Commerce, Justice, and State, the Judiciary, and Related Agencies*, 107th Cong. (2002) [hereinafter Mueller Testimony] (testimony of Robert S. Mueller, III, Director, FBI), https://www2.fbi.gov/congress/congress02/mueller062102.htm. "The Economic Espionage Unit is dedicated to countering the economic espionage threat to include developing training and outreach materials; participating in conferences; visiting private industry; working with law enforcement and intelligence community on requirement issues; and providing specific classified and unclassified presentations." *Investigative Programs Counterintelligence Division*, *supra*.

[24] As noted during a hearing before the House Judiciary Subcommittee on Crime while discussing the Economic Espionage Act bill, "threats to the nation's economic interest are threats to the nation's vital security interests." H.R. REP. NO. 104-788, at 4 (1996). Some, including former F.B.I. Director Louis Freeh, have called economic espionage "the greatest threat to [the United States] since the Cold War." Alan Gathright & Vanessa Hua, *Tech Theft Rises Amid China*

The FBI continually organizes training sessions and initiates working partnerships with the private sector to educate companies and universities as to potential weaknesses in their security systems whether these deficiencies be personnel and/or computer-related.[25] Their strategy of reaching out to the private sector, participating in seminars, round table discussions, making training films on the issue, and meeting with private industry stakeholders has been relatively successful in spreading the word as to damaging effects of economic espionage. [26]

---

*Ties*, S.F. CHRON. (Feb. 10, 2003), http://www.sfgate.com/news/article/Tech-theft-rises-amid-China-ties-Growing-2635355.php.

[25] *See* COVINGTON & BURLING LLP, *supra* note 21. *See also* U.S.-CHINA ECON. AND SEC. REV. COMM'N, 113TH CONG., REP. TO CONGRESS (Comm. Print 2013), http://origin.www.uscc.gov/Annual_Reports/2013-annual-report-congress.

[26] *Economic Espionage: A Foreign Intelligence Threat to American Jobs and Homeland Security: Hearing Before the Subcomm. on Counterterrorism and Intelligence of the H.R. Comm. on Homeland Security*, 112th Cong. 16–19 (2012) (statement of C. Frank Figliuzzi, Assistant Dir., Counterintelligence Div., Fed. Bureau of Investigation) [hereinafter Figliuzzi Testimony].

"To address the evolving Insider Threat, the FBI has become more proactive to prevent losses of information and technology. CD continues expanding our outreach and liaison alliances to government agencies, the defense industry, academic institutions, and, for the first time, to the general public, because of an increased targeting of unclassified trade secrets across all American industries and sectors. On May 11, 2012, the FBI launched a media campaign highlighting the Insider Threat relating to economic espionage. This campaign included print and television interviews, billboards along busy commuter corridors in nine leading research areas nationwide, and public information on the FBI Web site. Through this campaign, the FBI hopes to reach the public and business communities by explaining how the Insider Threat affects a company's operations and educating them on how to detect, prevent, and respond to threats to their organizations' proprietary information. Perhaps the most important among these is identifying and taking defensive measures against employees stealing trade secrets." *Id.*

"In February 2013, the Bureau held the first session of our National Cyber Executive Institute, a three-day seminar to train leading industry executives on cyber threat awareness and information sharing. One example of an effective public-private partnership is the National Cyber Forensics and Training Alliance, a proven model for sharing private sector information in collaboration with law enforcement. Located in Pittsburgh, the alliance includes more than 80 industry partners from a range of sectors, including financial services, telecommunications, retail and manufacturing. The members of the alliance work together with federal and international partners to provide real-time threat intelligence, every day. Another initiative the FBI participates in, the Enduring Security Framework, includes

Congress passed the Economic Espionage Act "(EEA)" in 1996[27] to much fanfare. The United States was tired of "the systematic pilfering of our country's economic secrets by our trading partners which undermines our economic security"[28] and wanted to communicate that we, as a society, morally condemn this type of crime—a crime that is punishable by a maximum of fifteen years in prison.[29] Prior to 1996, those stealing trade secrets were prosecuted using a variety of different federal statutes, including mail and wire fraud and the Interstate Transportation of Stolen Property.[30] However, the Supreme Court later ruled that trade secrets were not property, and thus, it was inappropriate to use the Interstate Transportation of Stolen Property statute to prosecute a number of these crimes.[31] Therefore, when former President Bill Clinton signed the Economic Espionage Act in 1996, it was the first time the FBI had a specific criminal statute with which to fight this particular problem.

The statute has since been amended to increase the fines that can be imposed, from $500,000 to $5 million in the case of an individual and from $10 million to not more than the greater of $10 million or three times the value of the stolen trade secret.[32] This reflects Congress' continued emphasis and focus on the severity of the crime.[33]

---

top leaders from the private sector and the federal government. This partnership illustrates that the way forward on cyber security is not just about sharing information, but also about solving problems together." *Threats to the Homeland: Hearing Before the Senate Comm. on Homeland Security and Governmental Affairs*, 113th Cong. 7–9 (2013) (statement of James B. Comey, Dir., Fed. Bureau of Investigation).

[27] Economic Espionage Act of 1996, Pub. L. No. 104–294, §101, 110 Stat. 3488 (1996).

[28] 142 CONG. REC. 14 (daily ed. Feb. 1, 1996) (statements of Sen. Kohl & Sen. Spector).

[29] 18 U.S.C. § 1831(a) (2012).

[30] 18 U.S.C. § 2314 (2012).

[31] Dowling v. United States, 473 U.S. 207, 215–18 (1985).

[32] Foreign and Economic Espionage Penalty Enhancement Act of 2012, Pub. L. No. 112-269, 126 Stat. 2442. (2013).

[33] EXEC. OFFICE OF THE PRESIDENT OF THE UNITED STATES, ADMINISTRATION'S WHITE PAPER ON INTELLECTUAL PROPERTY ENFORCEMENT LEGISLATIVE RECOMMENDATIONS 4 (2011), https://www.whitehouse.gov/sites/default/files/ip_white_paper.pdf [hereinafter ADMINISTRATION WHITE PAPER]. In 2011, the Administration recommended that "Congress increase the statutory maximum sentence for economic espionage [from 15 to] 20 years." In addition,

Title 18 United States Code Section 1831 (EEA) makes it a crime to knowingly steal or receive a trade secret for the benefit of any foreign government, foreign instrumentality, or foreign agent.[34] The term "trade secret" is described as "all forms and types of financial, business, scientific, technical, economic or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically or in writing."[35] Moreover, in order to be considered a trade secret, the owner must have "taken reasonable measures to keep such information secret" and the trade secret must have an independent economic value.[36] Trade secret examples include software, marketing plans, customer lists, source

---

the Administration asked Congress to direct the U.S. Sentencing Commission to consider increasing the guideline range based on aggravated offense conduct in theft of trade secret and economic espionage cases. *Id.* at 4–5

[34]

> (a) In General.— Whoever, intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly—
> (1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret:
> (2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret:
> (3) receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization:
> (4) attempts to commit any offense described in any of paragraphs (1) through (3); or
> (5) conspires with one or more other persons to commit any offense described in any of paragraphs (1) through (4), and one or more of such persons do any act to effect the object of conspiracy shall, except as provided in subsection (b), be fined not more than $500,000 or imprisoned not more than 15 years, or both.
> (b) ORGANIZATIONS. - Any organization that commits any offense described in subsection (a) shall be fined not more than $10,000,000.

Economic Espionage Act § 101, *supra* note 27.

[35] 18 U.S.C. § 1839(3) (2012).

[36] *Id.* Therefore, a trade secret is different from a patent or copyright whereby owners may sue under patent or copyright laws.

codes, pricing information, technical drawings, and chemical formulas.[37]

A foreign agent is defined as "any officer, employee, proxy, servant, delegate, or representative of a foreign government."[38] A foreign instrumentality is defined as "any agency, bureau, ministry, component, institution, or association, or any legal, commercial, or business organization, corporation, firm, or entity, that is substantially owned, controlled, sponsored, commanded, managed or dominated by a foreign government."[39]

The territorial limits of section 1831 are relatively broad. The EEA protects against theft that occurs either in the United States or outside the United States. If the theft occurs outside the United States, the violator must be a U.S. person or organization or an act in furtherance of the offense must have been committed in the United States.[40]

Since 1996, there have been six convictions under Section 1831.[41] On many occasions, an indictment was filed with a § 1831 charge included, but eventually the defendant pled guilty to a lesser charge such as § 1832 theft of trade secrets.[42] The following table summarizes the six § 1831 convictions:[43]

---

[37] *Do I Have Trade Secrets to Protect?*, MAX FILINGS (last visited Nov. 4, 2015), https://www.maxfilings.com/incorporation-knowledge-center/Trade-Secrets-to-protect.php.

Trade secrets are similar to trademarks, patents, and copyrights in that they are all deemed intellectual property, however, trade secrets do not share the same protections as the other three. Patents, trademarks, and copyrights all give the owners/creators an exclusive right to their work to distribute, copy, perform, display, modify, etc. World Intellectual Property Organization, *What is Intellectual Property?*, (last visited Oct. 24, 2015), http://www.wipo.int/edocs/pubdocs/en/intproperty/450/wipo_pub_450.pdf.

[38] 18 U.S.C. § 1839 (2012).

[39] *Id.*

[40] 18 U.S.C. § 1837 (2012).

[41] *A Look at 16 Years of EEA Prosecutions*, LAW 360 (Sep. 19, 2012 at 12:18 PM), http://www.law360.com/articles/378560/a-look-at-16-years-of-eea-prosecutions.

[42] *Id.*

[43] The author created this table by reading about these cases in the news. *See also* Offices of U.S. Att'ys, *Economic Espionage and Trade Secrets*, 57 U.S. ATT'YS BULL. (2009) and FBI, https://www.fbi.gov (last visited Apr. 19, 2016).

| Year | Case Name | Jurisdiction | Case Number | Company | Trade Secret | Foreign Entity | Country | Sentence |
|---|---|---|---|---|---|---|---|---|
| 2006 | United States v. Fei Ye & Ming Zhong | Court of Appeals for the Ninth Circuit | 436 F.3d 1117 (9th Cir. 2006) | NEC Electronics; Sun Microsystems Inc.; Transmeta Corporation | Microchip blueprints | Defendants' privately owned Chinese company | China | 1 year in prison |
| 2006 | United States v. Xiaodong Meng | Northern District of California | No. CR 04–20216 | Quantum3D, Inc. | nVSensor | Royal Thai Air Force, Royal Malaysian Air Force, & China's Navy Research Center | Thailand, Malaysia, & China | 24 months in prison |
| 2011 | United States v. Dongfan "Greg" Chung | Court of Appeals for the Ninth Circuit | 659 F.3d 815 (9th Cir. 2011) | Boeing | Aviation Technologies | China Aviation Industry Corp.; The People's Republic of China | China | 188 months in prison, and 3 years supervised release |
| 2011 | United States v. Kexue Huang | Southern District of Indiana | 2011 WL 6386398 | Dow AgroSciences; Cargill, Inc. | Biochemicals | Chinese University | China; Japan | 87 months in prison, 3 years of supervised release |
| 2011 | United States v. Elliot Doxer | District of Massachusetts | No. 1:11-CR-10268 (D. Mass. Dec. 21, 2011) | Akamai Technologies, Inc. | Customer and employee lists and contact information | Israeli Government | Israel | 6 months in prison, 2 years of supervised release, and a fine of $25,000 |
| 2014 | United States v. Walter Liew, & USA Performance Technology, Inc. | Northern District of California | 2014 WL 2586329 | E.I. du Pont de Nemours & Company ("DuPont) | Titanium Dioxide ("TiO2," used in Oreo® Whitening Recipe) | Pangang Group Limited Company | China | 15 years in prison and a fine of $511,667.82 |

Other criminal statutes have also been used in this area, to include theft of trade secrets (otherwise known as industrial espionage),[44] mail or wire fraud,[45] foreign or interstate transportation of stolen property[46], the Export Control Act[47] and the International Traffic in Arms Regulations (ITAR)[48], money laundering,[49] and the

[44] Section 1832 makes it a crime to knowingly perform targeting or acquisition of trade secrets or intend to convert a trade secret to knowingly benefit anyone other than the owner. 18 U.S.C. § 1832 (2012).

[45] 18 U.S.C. § 1341, (2012); 18 U.S.C. § 1343, (2012); 18 U.S.C. § 1346 (2012).

[46] 18 U.S.C. § 2314 (2012).

[47] 22 U.S.C. § 2778 (2012).

[48] 22 C.F.R. § 120. (2014).

[49] 18 U.S.C. § 1956, (2012); 18 U.S.C. § 1957 (2012).

Computer Fraud and Abuse Act Fraud Scheme.[50] Theft of trade secrets under § 1832 is easier to prosecute (hence the greater amount of convictions compared to § 1831) due to the fact that no government sponsorship (beneficiary) need be proven and the maximum sentence is ten years rather than fifteen years under § 1831. The number of theft of trade secrets convictions increased by more than sixty percent between 2009 and 2013.[51]

This reactive/prosecution part of the government's two-pronged strategy to combat economic espionage has had dismal results. The extremely small number of prosecutions has made only a minor, insignificant dent in what is a huge, ongoing problem. [52]

### B. *Other Nations' Responses*

While the United States remains the world's leader in research and development (R&D), and historically has been known for its innovation and cutting-edge technology, it is certainly not the only country to suffer from the consequences of economic espionage. In fact, most developed or developing countries have also been targeted for technology theft. Many countries have a number of criminal or civil statutes that can be applied when their government or private industry are victimized.[53] However, no country has a criminal statute with the specificity of §§1831 and 1832, which criminalize the theft of corporate trade secrets with the exception of Canada and New Zealand, but more countries are considering such legislation.[54] Not surprisingly, most foreign countries have a poor track record of successfully prosecuting acts of economic espionage.

---

[50] 18 U.S.C.A. § 1030 (2012). Intrusion or hacking is criminalized under 18 U.S.C. § 1030(a)(5).

[51] Coleman Statement, *supra* note 19. This article does not touch upon the civil trade secret enforcement statutes, 18 U.S.C. § 1838, or the Uniform Trade Secrets Act.

[52] "We're about high school soccer now; we've spread out, we pass well, but the bad guys are moving at World Cup speed, so we have to get better." Scott Pelley, *FBI Director On Threat of ISIS, Cybercrime*, CBS NEWS (Oct. 5, 2014), http://www.cbsnews.com/news/fbi-director-james-comey-on-threat-of-isis-cybercrime/.

[53] *See* table of various countries with applicable criminal statutes *infra*.

[54] *See* table of various countries with applicable criminal statutes *infra*. *See generally* GIBSON DUNN & CRUTCHER LLP, 2014 YEAR-END FRENCH LAW UPDATE 11 (2014), http://www.gibsondunn.com/publications/Documents/2014-Year-End-French-Law-Update.pdf.

The table below lists the various countries that have criminal statutes that can be applied to theft of trade secrets or economic espionage-type crimes:[55]

| Country | Criminal Statute | Year Created | Penalty | Benefit Requirement | Civil COA |
|---|---|---|---|---|---|
| Argentina | Code Pen. art. 159 | 1994/Amended 1996 | 1. Fines, which are adjusted for inflation;<br>2. Imprisonment from one month to one year; and possibly, where relevant<br>3. Legal disqualification from special professions from six months to three years. | Any third party, so long as it causes harm to the victim. | Yes |
| Brazil | Lei 9.279 | 1996/Amended 2013 | 1. Unspecified fines; or<br>2. Imprisonment for three months to one year. | Any third party | Yes |
| Canada | R.S.C. 1985, c. O-5 | 1989/Amended 2001 | 1. Imprisonment for no more than ten years. | Any third party | Yes |
| China | Law of September 2, 1993, of the People's Republic of China Against Unfair Competition (promulgated by People's Republic of China Presidential Order No. 10) | 1993/Amended 1997 | 1. Unspecified fines;<br>2. Imprisonment for no less than three years, but no more than seven years; and possible<br>3. Administrative sanctions | Any third party | Yes |

[55] The author compiled this table by referencing the above mentioned statutes as well as BRADLEY LIMPERT & OXANA IATSYK, LIMPERT: TECHNOLOGY CONTRACTING: LAW, PRECEDENTS AND COMMENTARY § 2-3 (2008).

| | | | | | |
|---|---|---|---|---|---|
| France | Protection of Trade Secrets through IPR and Unfair Competition Law § 14 | 1992/Amended 1996 | In cases where the act is committed concerning a database maintained by the French state that includes personal data:<br>1. Fines not to exceed €75,000 ($81,442.50); and<br>2. Imprisonment for five years.<br>In cases where national defense is compromised:<br>1. Fines not to exceed €100,000 ($108,590); and<br>2. Imprisonment for seven years.<br>In cases where infringer is employee:<br>1. Imprisonment of two years; and<br>2. Fines of €30,000.<br>In all other cases:<br>1. Fines not to exceed €45,000 ($48,865.50); and<br>2. Imprisonment for up to one year.<br>Supplementary sanctions may be imposed at the court's discretion:<br>1. Deprivation of voting rights;<br>2. Rights to be elected; and/or<br>3. Rights to be a guardian of a child. | Any third party | Yes |
| Germany | Act Against Unfair Competition §§ 15, 17 | 1909/Amended 2013 | In cases where one is an employee or former employee of the victim:<br>1. Unspecified fines; or<br>2. Imprisonment for up to three years.<br>In cases where one is obligated to keep the trade secret:<br>1. Unspecified fines; or<br>2. Imprisonment for up to two years. | Any third party, or with the intent of causing damage to the entrepreneur. | Yes |
| Italy | Penal Code, Arts. 622, 623 | 1996 | In cases where one acquired the secret through business:<br>1. Imprisonment for up to three years.<br>In all other cases:<br>1. Fines between €100 ($108.55) and €1000 ($1,085.52); or<br>2. Imprisonment for up to three years. | Any third party | Yes |

| | | | | | |
|---|---|---|---|---|---|
| Japan | Unfair Competition Prevention Law § 23 | 1991/Amended 2004 | 1. Imprisonment with labor for up to ten years; and/or<br>2. Fines not exceeding ¥10,000,000 ($82,529.40). In cases where one is an employee or former employee of the victim, the penalty also includes additional fines up to ¥300,000,000 ($2,476,332). | Any third party | Yes |
| Korea | Unfair Competition Prevention and Trade Secret Protection Act § 24 | 1992/Amended 2014 | 1. Imprisonment for up to ten years; or<br>2. Fines up to ₩100,000,000 ($89,703).<br>In cases where one is using the secret in order to benefit a foreign entity:<br>1. Imprisonment with labor for up to ten years; or<br>2. Fines equivalent to the amount ranging from not less than two times to not more than ten times the amount of the profit in property.<br>In all other cases:<br>1. Imprisonment with labor for up to five years; or<br>2. Fines equivalent to the amount ranging from not less than two times to not more than ten times the amount of the profit in property. | Any third party | Yes |
| Russia | Civil Code, Art. 139(1) | 1990/Amended 2014 | 1. Fines (which can include amount of defendant's income),<br>2. Imprisonment,<br>3. Deprivation of right to offices, or<br>4. Deprivation of rights to engage in certain activities.<br>Penalties are heightened if infringer is employee of victim. | Disclosure of information not legally available to third parties, including commercial, tax or banking secrets to any third party | Yes |
| Switzerland | Federal Act of December 19, 1986 on Unfair Competition | 1986/Amended 2014 | Imprisonment not to exceed three years and/or a monetary penalty. | Any external official agency, foreign organization, private enterprise, or agents of these. | Yes |
| Taiwan | Trade Secret Act | 1996/Amended 2013 | 1. Fines up to three times the amount of actual damages,<br>2. Injunctions, and/or 3. Imprisonment. | Infringer or any third party | Yes |
| UK | No criminal statute | - | No criminal penalties | Any unauthorized third party | Yes |

| | | | | | |
|---|---|---|---|---|---|
| United States | Economic Espionage Act of 1996, 18 U.S.C.A. § 1831 | 1996 | 1. Fines not to exceed $5 million and/or<br>2. Imprisonment not to exceed fifteen years. | Foreign Entity | No |

The countries that comprise the "Five Eyes,"[56] an intelligence alliance among the countries of Australia, Canada, New Zealand, the United Kingdom, and the United States, have varying ideas as to what should be done about economic espionage—Canada and New Zealand have similar criminal statutes to the U.S., the United Kingdom has previously considered passing such legislation, and Australia simply considers theft of trade secrets a civil matter.

### 1. CANADA

Canada has in place an almost mirror-image copy of the U.S.' EEA.[57] Richard Fadden, director of the Canadian Security Intelligence Service, stated in a report presented to Canadian parliament that state-sponsored espionage against Canada had reached "levels equal to, or greater than those witnessed during the Cold War."[58] The report indicated that Canada's "open society with strong international relationships and advanced industries such as telecommunications and mining—make it attractive to foreign intelligence agencies."[59] "As a world leader in communications, biotechnology, energy extraction technologies, aerospace and other areas, Canada remains an attractive target for economic espionage."[60]

---

[56] These five countries jointly coordinate their signals intelligence and are bound by the U.K./U.S. agreement to share such intelligence. *The Five Eyes*, Privacy International (last visited Nov. 4, 2015), https://www.privacyinternational.org/node/51.

[57] "Use of trade secret for the benefit of foreign economic entity – every person commits an offence who, at the direction of, for the benefit of or in association with a foreign economic entity, fraudulently and without color of right and to the detriment of Canada's economic interests, international relations or national defense or national security (a) communicates a trade secret to another person, group or organization; or (b) obtains, retains, alters or destroys a trade secret." Security of Information Act, R.S.C. 1985, c. O-5 (Can.).

[58] Agence France-Presse, *Canada's Spy Chief: Espionage Has Reached Cold War-Level*, RAW STORY (June 14, 2011, 4:51 PM), http://www.rawstory.com/2011/06/canadas-spy-chief-espionage-has-reached-cold-war-level/.

[59] *Id.*

[60] *Id.*

Canada has been targeted by both Russia and China. In 2012, two Russian diplomats were expelled from Canada in connection with an espionage case against a Canadian naval officer charged under the Security of Information Act, which accused the officer of giving "a foreign entity" secret information between 2007 and 2012.[61] The Security Act "carr[ies] a maximum penalty of life in prison."[62] Both Russia and Canada have an interest in the Arctic Circle where companies are exploring and mining for gold, diamonds, iron ore, lead, zinc, and uranium.[63]

That same year, Telvent Canada Ltd., an information technology company catering to the energy industry, stated that attackers had breached its internal firewall and security systems, installed malicious software, and had stolen project files related to a product that helps energy firms merge older IT assets with more advanced "smart grid" technologies.[64] Chinese hackers were blamed for the breach.[65] China also has mining exploration interests in the Arctic Circle.[66]

While Canada amended its Security of Information Act in 2001[67] to look incredibly similar to the United States' EEA, Canada has yet to complete such a prosecution under its laws.[68]

---

[61] *Russian Diplomats Left Canada Weeks Before Halifax Espionage Arrest*, NATIONAL POST (Jan. 20, 2012), [hereinafter *Russian Diplomats*], http://news.nationalpost.com/news/canada/russian-diplomats-left-canada-weeks-before-halifax-spy-mystery.

[62] *Id.*

[63] *Id*; David Ljunggren & Euan Rocha, *Mineral-Rich Canadian Arctic Territory Poised for Major Developments*, MINEWEB (Sept. 1, 2011), http://www.mineweb.com/archive/mineral-rich-canadian-arctic-territory-poised-for-major-developments/.

[64] Brian Krebs, *Chinese Hackers Blamed for Intrusion at Energy Industry Giant Telvent*, KREBS ON SECURITY (Sept. 26, 2012), http://krebsonsecurity.com/2012/09/chinese-hackers-blamed-for-intrusion-at-energy-industry-giant-telvent.

[65] *Id.*

[66] Ljunggren & Rocha, *supra* note 63.

[67] Section 19 of the Act makes it an offense for a person to "at the direction of, for the benefit of or in association with a foreign economic entity, fraudulently and without colour of right" communicate a trade secret to another person, group or organization or obtain, retain, alter or destroy a trade secret "to the detriment of" Canada's economic interests, international relations, national defense or national security. Security of Information Act, R.S.C. 1985, c. O-5 (Can.).

[68] A thorough review of the Security of Information Act, R.S.C. 1985, c. O-5 (Can.) indicates no convictions under Section 19 have occurred.

### 2. NEW ZEALAND

New Zealand amended its Crimes Act in 2003 and made intellectual property/trade secret theft a crime in Section 230.[69] The language used in Section 230, "taking, obtaining, or copying of trade secrets," looks similar to the United States' theft of trade secrets offense under Section 1832.[70] "The intent elements require intent to obtain any pecuniary advantage or to cause loss to any other person, and acting dishonestly and without claim of right."[71] Legislative history suggests that foreign economic espionage was a primary concern in passing the legislation.[72] Despite its passage, its fate has gone the way of Canada with Section 230 having been "little used" and not used at all in the foreign economic espionage context.[73] In fact, one law professor in New Zealand, Anna Kingsbury, argues that the problem could be dealt with in the civil legal system and that such a crime only encourages protection, reduces competition, and inhibits innovation and employee mobility.[74] Kingsbury sees an economic espionage crime as "based in an idea of inter-country competition that does not fit well with contemporary understandings of the economics of trade and theories of comparative advantage."[75] Thus, in a "global" marketplace, employees that steal trade secrets are actually assisting in competition and innovation on a "global" level. New Zealand's Section 230 has yet to be tested.

### 3. UNITED KINGDOM

In the United Kingdom (UK), "[t]here is no statute in English criminal law that is specifically aimed at penalizing a person who misuses another's trade secrets."[76] Moreover, the crime of theft

---

[69] Anna Kingsbury, *Trade Secret Crime in New Zealand Law: What Was the Problem and Is Criminalization the Solution?*, 37 Eur. Intell. Prop. Rev. 147, 149 (2015). "Section 230 of the Crimes Act 1961 as amended in 2003 provides for an offence of taking, obtaining or copying trade secrets. The penalty on conviction is imprisonment for up to five years." *Id.*

[70] *Id.*; 18 U.S.C. § 1832 (2012).

[71] Kingsbury, *supra* note 69, at 149.

[72] *Id.* at 151.

[73] *Id.* at 151–52.

[74] *Id.* at 152.

[75] *Id.* at 153.

[76] 3 HILARY PEARSON, TRADE SECRETS THROUGHOUT THE WORLD § 39:19 (2014).

would rarely apply, as confidential information does not fall within the definition of "property."[77] "In the non-criminal context, however, English law [particularly breach of confidence] provides broad and effective protection for trade secrets through a variety of available remedies. These remedies include: search and seizure orders, injunctive relief, damages, accounting for profits, third party liability, constructive trusts over assets acquired as a result of the breach and an order to reveal the source of the disclosed information."[78]

One consultation paper created by the UK Law Commission recommended that the UK criminalize the theft of trade secrets and suggested that the discussion was forthcoming in Parliament:

We provisionally conclude that the main arguments in favour of criminalizing trade secret misuse are as follows:

> (1) That there is no distinction in principle between the harm caused by such misuse and the harm caused by theft;
>
> (2) That the imposition of legal sanctions is necessary in order to protect investment in research;
>
> (3) That civil remedies alone are insufficient to discourage trade secret misuse (and would continue to be insufficient if exemplary damages were made more widely available), because many wrongdoers are unable to satisfy any judgment against them; infringement of copyright and registered trademarks but not the misuse of
>
> (4) That is inconsistent for the law to prohibit the trade secrets; and
>
> (5) That criminalization would help to preserve standards in business life.[79]

---

[77] *Id.*; see Theft Act of 1968, c. 60, § 4 (Gr. Brit.).

[78] BRADLEY LIMPERT & OXANA IATSYK, LIMPERT: TECHNOLOGY CONTRACTING: LAW, PRECEDENTS AND COMMENTARY § 2-3(c)(i) (2008).

[79] GREAT BRITAIN: LAW COMMISSION, LEGISLATING THE CRIMINAL CODE: MISUSE OF TRADE SECRETS – A CONSULTATION PAPER 30 (1997).

However, these suggestions were not acted upon. The UK also proposed changes to the Serious Crime Bill in order to deter hackers by increasing the penalty under the Computer Misuse Act to a life sentence.[80]

### 4. AUSTRALIA

To date, Australia has not decided to follow the example set by the United States and criminalize acts of economic espionage. Australia relies upon civil and contractual enforcement through "breach of confidence" which has its roots in English law.[81] Also, as a signatory to the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), Australia has an international obligation under Article 39(2) to protect undisclosed information that has commercial value because it is secret though it has no specific trade secret protection laws on the books.[82]

Gillian Dempsey, a lecturer at the Australian National University, argues that despite the lack of protection, Australia's regulation of trade secrets is not deficient.[83] Dempsey tends to agree with her New Zealand counterpart that "[i]n a modern economy, production tends to be characterized by alliances between firms" in order to cut down on R&D costs and therefore alliances and sharing with firms "already possessing the requisite complementary knowledge" can be an "efficient manner of solving a problem involving specialist knowledge."[84] Criminalizing the theft of trade secrets may reduce any incentive a company might have to cooperate and share with others.[85]

Moreover, Dempsey argues that companies should be responsible for their own security interests and should not burden the government with these sorts of costs.

---

[80] Lee Munson, *Hackers Who Threaten National Security Could Face Life Sentences*, NAKED SECURITY (Oct. 24, 2014), https://nakedsecurity.sophos.com/2014/10/24/hackers-who-threaten-national-security-could-face-life-sentences/.

[81] Gillian Dempsey, *Industrial Espionage: Criminal or Civil Remedies*, AUSTL. INST. CRIM., Mar. 1999, at 1, 3–4.

[82] 1 RICHARD GOUGH, TRADE SECRETS THROUGHOUT THE WORLD § 2:2 (West 2014).

[83] Dempsey, *supra* note 81, at 4.

[84] *Id.* at 5.

[85] *See id.*

> [T]o argue for criminalization would involve an implicit assumption that the interest of the firm is concurrent with the interest of society as a whole. The costs of detection and policing are likely to be relatively higher in a criminal arena than in a civil arena. . . . And the policing agency would have to acquire sufficient experience and knowledge in information security and evidence gathering techniques in a market where such knowledge is at a premium.[86]

In Dempsey's argument, only the company whose trade secrets are being protected would benefit, and the rest of society, in contrast, would suffer the "disastrous" consequences on "innovation and competitiveness."[87]

### 5. JAPAN

Japan is thoroughly aware of the economic espionage problem. Nissan acknowledged it might have been hacked in April 2012 when they detected the presence of a computer virus on their network, and they believed user IDs and passwords had been transmitted to hackers who "were looking for intellectual property related to its EV drivetrains."[88] "Japan's Finance Ministry . . . uncovered evidence of a major Trojan cyber-attack on its computer systems [in order to steal confidential information in 2010 and 2011 that remained] undetected for almost two years."[89]

In 2012, "three IT executives were arrested in Japan for . . . allegedly us[ing] Android malware to 'earn' themselves over 20 million yen[90] from unsuspecting victims" that downloaded a video

---

[86] *Id.* at 6.

[87] *Id.*

[88] Shane McGlaun, *Nissan Gets Hacked, Target Could've Been Intellectual Property*, DAILY TECH (Apr. 24, 2012), http://www.dailytech.com/Nissan+Gets+Hacked+Target+Couldve+Been+Intellectual+Property/article24527.htm.

[89] John Dunn, *Japan's Finance Ministry Uncovers Major Trojan Attack*, CSO ONLINE (July 24, 2012), http://www.csoonline.com/article/711878/japan-s-finance-ministry-uncovers-major-trojan-attack.

[90] Twenty million yen is equivalent to approximately half a million U.S. dollars.

playing application.[91] "Once downloaded and run, it would badger the users by requesting them to pay a 99,800 yen (around $1,256) fee every few minutes, in addition to stealing their personal data and storing it on a remote server for future use."[92] Japan had recently introduced a law that makes malware creation and distribution a criminal act.[93]

Japan has taken several steps to improve its efforts to counter industrial espionage. Prior to 2009, the government was required to prove that the trade secret theft resulted in profits for a third party beneficiary.[94] Japan has since revised its Unfair Competition Prevention Law so that it need only prove that the person committing industrial espionage took information from a company without permission.[95] In 2014, the Japanese government formed a committee made up of government and company executives to discuss ways to prevent trade secret theft and improve communication between government investigators and private companies.[96] Before this committee, there had been little coordination and information sharing between investigative authorities and companies, and investigators were unable to start an investigation unless a company filed a complaint.[97] Japanese executives are reticent to disclose any type of theft as that would mean they would have to take full responsibility for the loss and "reporting may cause further time commitments and expenses."[98]

It must also be said that Japan has been known to conduct its own economic espionage. Japanese industry is promoted by its own government; the Ministry of Economic Trade and Industry (METI) uses the Japan External Trade Office (JETRO) to collect economic

---

[91] Zeljka Zorz, *Six Arrested for Peddling Android Malware in Japan*, NET SECURITY (June 18, 2012), http://www.net-security.org/malware_news.php?id=2147.

[92] *Id.*

[93] *Id.*

[94] *Gov't Eyes Panel to Share Info on Industrial Espionage*, THE DAILY YOMIURI, Jan. 15, 2014.

[95] *Id.*

[96] *Id.*

[97] *Id.*

[98] *Id.*

and trade information.[99] JETRO, interestingly enough, offers free commercial space and free communications to foreign companies in downtown Tokyo.[100]

### 6. LATIN AMERICA

Latin America has also been facing an upsurge in cybercrime. According to a 2013 report by Trend Micro and the Organization of American States (OAS), cyberattacks increased between "8 to 40 percent in Latin America and the Caribbean."[101] "A lack of cybercrime laws, economic challenges, and unpatched and unprotected citizen machines make the region ripe for cybercrime—and the data only represents a fraction of the cybercrime incidents there since few incidents are even reported or detected."[102] "Attacks on critical infrastructure, [industrial control systems, and financial institutions] are on the rise."[103]

While Latin America may not have a history of intellectual property protection, countries such as Argentina, Brazil, and Mexico have "paved the legal road with legislation aimed to protect industrial or commercial confidential information."[104]

## III. THE LEADING OFFENDERS OF ECONOMIC ESPIONAGE

Some of those countries listed in the table that consider economic espionage a crime are also some of the greatest perpetrators of trade secret theft. Many foreign intelligence services feed their pilfered information to domestic companies, thereby giving them a competitive edge over other foreign companies.[105] "[T]he leading

---

[99] U.N. CONF. ON TRADE AND DEVELOPMENT SECRETARIAT, REP. INTERNATIONAL TRADE AFTER THE ECONOMIC CRISIS 8 (Nov. 15, 2010) http://unctad.org/en/Docs/ditctab20102_en.pdf.

[100] *A Free Office in Tokyo*, VENTURE JAPAN, http://www.venturejapan.com/fast-track-starting-business-6.htm.

[101] Kelly Jackson Higgins, *Threat Nuevo: Latin America, Caribbean Cybercrime on the Rise*, DARK READING (May 3, 2013), http://www.darkreading.com/vulnerabilities---threats/threat-nuevo-latin-america-caribbean-cybercrime-on-the-rise/d/d-id/1139676?.

[102] *Id.*

[103] *Id.*

[104] *See* LIMPERT & IATSYK, *supra* note 78 § 2.3(b).

[105] Cotriss, *supra* note 8.

state intelligence threats [are said] to be Russia and China, based on their capabilities, intent, and broad operational scopes."[106] However, there are certainly other players waiting to take China and Russia's place.[107]

### A. *China*

> [T]here are two kinds of big companies in the United States[: t]hose that have been hacked by the Chinese and those who don't know they've been hacked by the Chinese.[108]

—FBI Director James Comey

China first enacted trade secret "protections" in 1993 with the passage of Article 10 of the Unfair Competition Law, which prohibits businesses from the following:

> a) obtaining the trade secret of the rightful party by theft, inducement, duress or other illegal means; b) disclosing, using or allowing others to use the trade secrets of the rightful party obtained by illegal means; or c) disclosing, using or allowing others to use trade secrets in breach of an agreement or the

---

[106] *Worldwide Threat Assessment of the U.S. Intelligence Community: Hearing Before Senate Armed Services Comm.*, 114th Cong. 4 (2015) (statement for the record of James R. Clapper, Director of National Intelligence), http://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf.

[107] "A growing number of computer forensic studies by industry experts strongly suggest that several nations—including Iran and North Korea—have undertaken offensive cyber operations against private sector targets to support their economic and foreign policy objectives, at times concurrent with political crises." *Id.* at 1.

[108] Pelley, *supra* note 52. China denies that it targets U.S. companies. "[PRC] Foreign Ministry spokesman Liu Weimin reportedly said in a statement that China's rapid ascendancy in terms of its military and space achievements are not down to cyber espionage but the 'pioneering, innovative and devoted work' of the Chinese people." Phil Muncaster, *China Hits Back at U.S. Cyber Snooping Allegations*, REGISTER (Apr. 23, 2012), http://www.theregister.co.uk/2012/04/23/us_china_spying_satellite/.

> confidentiality requirement imposed by the rightful party.[109]

Criminal sanctions, which may include up to seven years of imprisonment, may be used if the following three elements are met: "(a) gross violation of the rights; (b) serious circumstances; and (c) a large amount of illegal income, with heavy losses being suffered by the victim."[110]

Despite these so-called protections, China aggressively pursues foreign companies' trade secrets and intervenes to support Chinese businesses against foreign competitors. In fact, the National People's Congress in 2011 approved a five-year economic plan which mirrored most of the common targets of Chinese cyberspying: clean energy, biotechnology, advanced semiconductors, information technology, high-end manufacturing, such as aerospace and telecom equipment, and biotechnology, including drugs and medical devices.[111] China also wants U.S. technology, in particular, to advance their own military needs.[112]

In 2010, China surpassed Japan as the world's second largest economy.[113] One of the main reasons the Chinese economy has flourished is due to the fact Chinese companies have been able "to skip over [or accelerate] costly and time-consuming R&D and bring products to market using U.S. trade secrets, technology and IP."[114]

China appears to use the vacuum cleaner approach—collect it all. China has accounted for roughly 50 to 80% of all open economic espionage and trade secret theft investigations in the United States alone.[115] Their common methods of economic espionage can be di-

---

[109] *See* LIMPERT & IATSYK, *supra* note 78 § 2.3(e)(ii) (2008).

[110] *Id.*

[111] Riley & Walcott, *supra* note 11. *See also* KPMG INTERNATIONAL, CHINA'S 12TH FIVE-YEAR PLAN: CONSUMER MARKETS 2 (2011), http://www.kpmg.com/cn/en/IssuesAndInsights/ArticlesPublications/Documents/China-12th-Five-Year-Plan-Consumer-Markets-201104.pdf.

[112] Cotriss, *supra* note 8.

[113] Justin McCurry and Julia Kollewe, *China Overtakes Japan as World's Second-Largest Economy*, GUARDIAN (Feb. 14, 2011, 1:38 PM), http://www.theguardian.com/business/2011/feb/14/china-second-largest-economy [hereinafter *China Overtakes Japan*].

[114] Cotriss, *supra* note 8.

[115] COMM'N ON THEFT AM. INTELL. PROP., *supra* note 10, at 15.

vided into three categories: (1) hacking; (2) recruiting students, business executives, and insiders overseas to steal trade secrets; and (3) stealing from businesses who choose to manufacture in or conduct joint ventures with China.

### 1. HACKING AND THE PEOPLE'S LIBERATION ARMY

In the case of China, it is relatively easy to prove the EEA's foreign government/instrumentality/agent nexus. In December 2011, the Wall Street Journal reported that the Chinese military sponsors most of the Chinese cyberspying.[116] "The Chinese cyberspying campaign stems largely from a dozen groups connected to China's People's Liberation Army and a half-dozen nonmilitary groups connected to organizations like universities . . . "[117]

In May 2013, the Washington Post described a classified report by the Defense Science Board, which listed more than 24 U.S. weapon system designs the board determined were accessed by cyber intruders.[118] "[S]enior military and industry officials with

---

[116] Siobhan Gorman, *United States Homes In on China Spying*, WALL STREET J., (Dec. 13, 2011), http://www.wsj.com/articles/SB10001424052970204336104577094690893528130.

[117] *Id.* "The Chinese government, primarily through the PLA and the [Ministry of State Security], supports these activities by providing state-owned enterprises information and data extracted through cyber espionage to improve their competitive edge, cut R&D timetables, and reduce costs. The strong correlation between compromised U.S. companies and those industries designated by Beijing as 'strategic' industries further indicates a degree of state sponsorship, and likely even support, direction, and execution of Chinese economic espionage. Such governmental support for Chinese companies enables them to out-compete U.S. companies, which do not have the advantage of leveraging government intelligence data for commercial gain." Larry M. Wortzel, *China's Military Modernization and Cyber Activities: Testimony of Dr. Larry M. Wortzel Before the House Armed Services Committee*, 8 Strategic Studies Quarterly 3, 14 (2014).

[118] Ellen Nakashima, *Confidential Report Lists U.S. Weapons System Designs Compromised by Chinese Cyberspies*, WASH. POST (May 27, 2013), http://www.washingtonpost.com/world/national-security/confidential-report-lists-us-weapons-system-designs-compromised-by-chinese-cyberspies/2013/05/27/a42c3e1c-c2dd-11e2-8c3b-0b5e9247e8ca_story.html.

knowledge of the breaches said the vast majority were part of a widening Chinese campaign of espionage against U.S. defense contractors and government agencies."[119]

"[C]yberspies hacked into the computer networks of POSCO, the South Korean steel giant in July 2006. . . . the same month that the steelmaker, the third largest in the world, initiated a takeover of a large steel mill in eastern China."[120] Mandiant, a private security firm, issued a report in 2014 called "APT1" that accused China's PLA of launching cyberespionage attacks against 141 companies in 20 industries through a group known as "PLA Unit 61398" operating mainly from Shanghai.[121] "The PLA . . . passes such information to Chinese companies . . . so they can rapidly increase their own capabilities."[122]

"[PLA] leaders have embraced the idea that successful war fighting is based on the ability to exert control over an adversary's information and information systems. The PLA has placed computer network operations in a unified framework broadly known as information confrontation and seeks to integrate all elements of information warfare, electronic and non-electronic, offensive and defensive, under a single command authority."[123]

---

[119] *Id.* The list included the Patriot missile system, the Aegis ballistic missile defense system, the F/A-18 fighter, the V-22 Osprey multirole combat aircraft, and the Littoral Combat Ship. *Id.*

[120] Riley & Walcott, *supra* note 11.

[121] Ellen Mesmmer, *Chinese Government Still Sponsoring Cyber-Espionage, says FireEye COO*, CHANNELWORLD (Mar. 3, 2014), http://specials.channelworld.in/channel_news/chinese-government-still-sponsoring-cyber-espionage,-says-fireeye-coo.

[122] Rick Newman, *China May Have Hacked Your Company, Too*, YAHOO FINANCE (May 20, 2014), http://finance.yahoo.com/blogs/daily-ticker/china-has-probably-hacked-your-company--too-175016269.html.

[123] Press Release, U.S.-China Econ. and Sec. Rev. Comm'n, Chinese Capabilities for Computer Network Operations and Cyber Espionage (March 8, 2012), http://origin.www.uscc.gov/sites/default/files/USCC%20Report%20-%20Chinese%20Capabilities%20for%20Computer%20Network%20Operations%20and%20Cyber%20Espionage.pdf. "The Chinese military's close relationship with large Chinese telecommunications firms creates an avenue for state sponsored or state directed penetrations of supply chains for electronics supporting U.S. military, government, and civilian industry—with the potential to cause the catastrophic failure of systems and networks supporting critical infrastructure for national security or public safety." *Id.*

"Some Chinese hacker groups, including groups affiliated with the PLA, will carry out their official missions during the day and then hack for profit at night. Other hacking groups will come across commercially valuable information as they carry out their official espionage tasks, take it, and then sell it for a personal profit to Chinese firms. Economic espionage is a money making activity for the PLA, and this increases the difficulty of bringing it under control."[124]

"China's leaders describe modernization of the PLA as essential to preserving and sustaining what they view as a 'period of strategic opportunity' to advance China's national development during the first two decades of the 21st century. China's leaders see this period as providing an opportunity to focus on fostering a stable external environment to provide the PRC the strategic space to prioritize economic growth and development and to achieve 'national rejuvenation' by 2049."[125]

### 2. STUDENTS AND INSIDERS

China's "energetic espionage program . . . began with China's economic opening to the West in the early 1980s and moved into cyberspace at least twelve years [ago.]"[126] "In 1986, Deng Xiao Peng established 'Program 863,' a sort of academy of sciences and technologies charged with closing the scientific gap between China and the world's advanced economies in a very short period of time.

---

[124] *China's Military Modernization and its Implications for the United States: Hearing Before U.S.-China Econ. and Sec. Rev. Comm'n*, 113th Cong. 72–81 (2014) (statement of James A. Lewis, Director and Senior Fellow of Strategic Technologies Program, Center for Strategic and International Studies) [hereinafter Lewis Statement].

[125] DEP'T OF DEFENSE, ANNUAL REPORT TO CONGRESS: MILITARY AND SECURITY DEVELOPMENTS INVOLVING THE PEOPLE'S REPUBLIC OF CHINA 2014, i (2014) [hereinafter ANNUAL REPORT TO CONGRESS 2014], http://www.defense.gov/Portals/1/Documents/pubs/2014_DoD_China_Report.pdf. The PLA's "New Historic Missions" codified in a 2007 amendment to the Chinese Communist Party (CCP) Constitution are to "[p]rovide an important guarantee of strength for the CCP to consolidate its ruling position"; "[p]rovide a strong security guarantee for safeguarding the period of strategic opportunity for national development"; "[p]rovide a powerful strategic support for safeguarding national interests"; and "[p]lay an important role in safeguarding world peace and promoting common development." *Id.* at 16.

[126] Lewis Statement, *supra* note 124, at 77–78.

The 863 Program and its institutional derivatives not only sponsored actual research, they also promoted the acquisition of advanced technologies from other countries legally or illegally."[127] The PRC uses its citizens studying and working abroad to collect trade secrets and bring them back to the motherland.[128]

Deng Xiaoping once said, "[w]hen our thousands of Chinese students abroad return home, you will see how China will transform itself."[129]

In 2009, the U.S.-China Economic and Security Review Commission quoted testimony provided by former FBI Special Agent I.C. Smith that:

> The Ministry of State Security sometimes places pressure on Chinese citizens going abroad for educational or business purposes and may make pursuit of foreign technology a quid pro quo for permission to travel abroad. However, this phenomenon of "entrepreneurial espionage" appears to be particularly common among businessmen who have direct commercial ties with Chinese companies and who seek to skirt U.S. export control and economic espionage laws in order to export controlled technologies to the PRC. In such instances, profit appears to be a primary motive, although the desire to "help China" can intersect in many cases with the expectation of personal financial gain.[130]

The greatest attribute of Chinese scholars in the eyes of the PRC is their vulnerability to the Communist Party's control. If bribes and

---

[127] William Pentland, *Entrepreneurial Espionage—Made in China*, FORBES (Jan. 22, 2011,), http://blogs.forbes.com/williampentland/2011/01/22/entrepreneurial-espionage-made-in-china/.

[128] U.S.-CHINA ECON. AND SEC. REV. COMM'N, 111TH CONG., REP. TO CONGRESS (Comm. Print 2009), [hereinafter U.S.-CHINA REP. TO CONGRESS 2009], http://www.uscc.gov/sites/default/files/annual_reports/2009-Report-to-Congress.pdf. According to Chinese official's statistics, in 2000 there were 190,000 PRC students in the United States. SUJIAN GUO AND BAOGANG GUO, THIRTY YEARS OF CHINA-U.S. RELATIONS 106 (Lexington Books, 2010).

[129] Robert Lenzer, *The China Hand*, FORBES (Oct. 31, 2005), http://www.forbes.com/forbes/2005/1031/079.html.

[130] U.S.-CHINA REP. TO CONGRESS 2009, *supra* note 128, at 160.

appeals to nationalism do not persuade students to spy for China, coercion usually does. Beijing can easily coerce students to cooperate by threatening their visa status, tuition scholarships, future career, and even their families living in China.[131]

Insider "spies" are also comprised of a significant group of business executives who chose to steal trade secrets from their company for monetary or ideological reasons. Much of the information stolen is dual-use technology, which assists China in rapidly increasing its military capabilities.[132] In *United States v. Chung*, an insider's interaction with the Western aviation-manufacturing firm, Boeing, provided a huge benefit to China's defense aviation industry.[133] Moreover, it is estimated that China has "over 3,000 front companies [operating] in the United States," some with the sole purpose of facilitating technology transfer to China.[134]

### 3. JOINT BUSINESS VENTURES WITH CHINA

National industrial policy goals in China encourage intellectual property (IP) theft, and an extraordinary number of Chinese business and government entities are engaged in this practice. "There are also weaknesses and biases in the legal and patent systems that lessen the protection of foreign [IP while] other policies . . . favor domestic suppliers," particularly in the technology field.[135]

---

[131] *Id.* at 7, 12, 160–66.

[132] DEP'T OF DEFENSE, ANNUAL REPORT TO CONGRESS: MILITARY AND SECURITY DEVELOPMENTS INVOLVING THE PEOPLE'S REPUBLIC OF CHINA 2012, at 10 (2012) [hereinafter ANNUAL REPORT TO CONGRESS 2012], http://www.defense.gov/Portals/1/Documents/pubs/2012_CMPR_Final.pdf. "One of the PRC's stated national security objectives is to leverage legally and illegally acquired dual-use and military-related technologies to its advantage. China has had a long history of cooperation between its civilian and military sectors and openly espouses the need to exploit civilian technologies for use in its military modernization. In this context, the cumulative effect of U.S. dual-use technology transfers to China could also make a substantial material contribution to its military capabilities." *Id.*

[133] United States v. Chung, 659 F.3d 815 (9th Cir. 2011).

[134] CARL ROPER, TRADE SECRET THEFT, INDUSTRIAL ESPIONAGE, AND THE CHINA THREAT 81 (2014).

[135] Eric Chabrow, *Panel: Use Hack-Back to Mitigate IP Theft*, BANK INFO SECURITY (May 23, 2013), http://www.bankinfosecurity.com/panel-hack-back-or-sorts-to-shield-ip-a-5784.

Since the 1980s, Chinese business partners have demanded that some sort of technology transfer occur as part of every major business negotiation.[136] "Foreign Direct Investment (FDI) has been the largest source of technology transfer for China."[137] "When western aircraft companies create co-production facilities in China, they teach Chinese workers how to build planes to western standards."[138]

Any foreign company working within China or conducting business with China needs to understand that Chinese intelligence organizations and other state entities are behind the plots to steal their technology.[139] Chinese state-owned businesses are among some of the largest firms in the world.[140] The U.S.-China Economic Review Commission Report of 2011 indicated that China's privatization reforms have, in some cases, reversed gains by the private sector and the state sector is strengthening.[141] The state-owned Assets Supervision and Administration Commission (SASAC) is the controlling shareholder of some 120 state-owned firms, and the SASAC controls $3.7 trillion in assets.[142] China's state-owned enterprises receive a variety of benefits and include "preferred access to bank capital, below-market interest rates on loans from state-owned banks, favorable tax treatment, policies that create a favorable competitive environment for SOEs relative to other firms and large capital injections when needed."[143] "In fact, the state has the preponderance of control over individual cyber rights. This permits the Chinese government to act freely regarding the management of information or

---

136 Lewis Statement, *supra* note 124, at 79–80.

137 *Id.* at 3.

138 *Id.*

139 Pentland, *supra* note 127.

140 U.S.-CHINA ECON. AND SEC. REV. COMM'N REPORT TO CONGRESS, 112TH CONG., 44–45 (2011), http://origin.www.uscc.gov/sites/default/files/annual_reports/annual_report_full_11.pdf [hereinafter U.S.-CHINA REP. TO CONGRESS 2011] ("In 2010, of 42 mainland Chinese companies listed in the Fortune Global 500, all but three were state owned. By revenues, three Chinese state-owned companies ranked among the top ten in the Fortune Global 500, compared to just two American companies.").

141 *Id.*

142 *State Capitalism in China: of Emperors and Kings*, ECONOMIST (Nov. 12, 2011), http://www.economist.com/node/21538159.

143 U.S.-CHINA REP. TO CONGRESS 2011, *supra* note 140, at 2.

its monitoring. The Chinese can establish their own rules for anything they claim to own."[144]

Moreover, the theft of trade secrets is not only promoted by government policies and state-backed companies, but it also reflects the societal attitude towards intellectual property. "One reason China does not have a strong domestic software industry, for example, is that no Chinese company can survive the wholesale pirating of its products."[145] Microsoft estimates that only one out of every ten customers using its software in China is paying for it.[146] But conditions are improving.[147] The percentage of pirated software usage in China dropped to 77% in 2011.[148]

Guy Sorman, a French journalist who spent two years traveling throughout China and interviewing various people, wrote:

> Whether it's electronics, garments, consumer durables, or cars, Chinese firms are content to assemble, subcontract, or recopy. At times, they respect intellectual property, though generally it is ignored. Piracy is the norm. Enter any shop in China and you can get the imitation of any Western luxury or electronic good at half the price. . . .
>
> This has become a source of great concern for Western firms. Because this illegal trade is virtual, there is no way of controlling it. The ingenuity of Chinese piracy knows no bounds. In the summer of 2005, the bookstores of mainland China were selling the seventh volume of the Harry Potter series even before it had been written by its British author. In defense of the Chinese counterfeiter, imitation is part of a long

---

144 Timothy L. Thomas, *Google Confronts China's "Three Warfares,"* 40 PARAMETERS 101, 111 (2010).

145 Lewis Statement, *supra* note 124, at 78–9.

146 Jon Brodkin, *Ballmer to Hu: 90% of Microsoft customers in China using pirated software*, NETWORK WORLD (Jan 21, 2011 12:15 PM), http://www.networkworld.com/article/2199038/software/ballmer-to-hu--90--of-microsoft-customers-in-china-using-pirated-software.html.

147 Cyrus Lee, *Report: China's Software Piracy Rate Falls to New Low – of 77%*, ZD NET (May 17, 2012, 12:31 PM), http://www.zdnet.com/article/report-chinas-software-piracy-rate-falls-to-new-low-of-77/.

148 *Id.*

> tradition. As far back as the 1660s, the Spanish missionary Navarrete had observed that the Cantonese artisans were "past masters in the art of counterfeiting, selling in China as the genuine article the fakes they had copied from the West."
>
> . . . The concept of intellectual property has no meaning for Chinese producers, who see it as yet another form of Western protectionism. There is a School of Intellectual Property at the University of Shanghai. Its director, responsible for educating future Chinese entrepreneurs, says: "International brands are far too expensive. Their high price excludes most of mankind from the benefits of the world economy." In other words, intellectual property is theft, and pirates are philanthropists . . . .
>
> Some may argue that Korea and Japan experienced a similar phase before they managed to set up systems and produce brands of international repute. China, too, may replicate the same virtuous cycle. Such a development does not seem likely in the near future, however. China lacks innovation not because it is a new economy but because its institutions do not foster the innovative spirit.[149]

### B. *Russia*

While China uses various methods to steal foreign trade secrets for both political and economic interests,[150] Russia has recently focused its efforts on cyber espionage to promote its national economic interests, while also employing intelligence officers under

---

[149] GUY SORMAN, EMPIRE OF LIES: THE TRUTH ABOUT CHINA IN THE TWENTY-FIRST CENTURY 107–108 (Asha Puri trans., Encounter Books 2008).

[150] Jim Finkle, *Russia Hacked Hundreds of Companies, Says Security Firm*, REUTERS (Jan. 22, 2014, 7:58 AM), http://www.haaretz.com/news/world/1.569913. *See also* Piore, *supra* note 11 ("In the late 1980s, the German hacker Markus Hess and several associates were recruited by the KGB to penetrate computers at American universities and military labs. They made off with sensitive semiconductor, satellite, space, and aircraft technologies").

diplomatic cover.[151] A U.S. cybersecurity firm, Crowdstrike, reported this past year that Russia has spied on "hundreds of American, European and Asian companies" to include "European energy companies, defense contractors, technology companies . . . manufacturing and construction firms in the United States, Europe and the Middle East as well as U.S. healthcare providers."[152]

"Russia's intelligence services are conducting a range of activities to collect economic information and technology from U.S. targets" in particular.[153] Because Russia relies mainly on hacking to accomplish its goals, it is much more difficult to prove which attacks are government sponsored and where the source of the attacks originated.[154] Foreign intelligence services, such as the Russian Foreign Intelligence Service ("SVR"), have used independent hackers as proxies, thereby giving the agencies plausible deniability.[155]

---

[151] The FBI estimates that approximately 25% of all diplomats in the United States are intelligence officers or affiliated with a foreign intelligence service. DEP'T OF JUSTICE, SUMMARY OF MAJOR U.S. EXPORT ENFORCEMENT, ECONOMIC ESPIONAGE, TRADE SECRET AND EMBARGO-RELATED CRIMINAL CASES (2015). The Czech secret service, Security Information Service (BIS), released a report this year stating that "[b]oth the Russian and Chinese embassy employ intelligence officers serving under diplomatic cover." In 2013, the number of such officers at the Russian embassy was "extremely high" according to BIS. Jan Lopatka & Catherine Evans, *Czech Secret Service Sees 'Extremely High' Number of Russian Spies*, REUTERS (Oct. 27, 2014, 8:30 AM), http://www.reuters.com/article/2014/10/27/us-czech-russia-espionage-idUSKBN0IG17B20141027 (quoting the BIS report that stated "[r]ussian intelligence services attempted to make use of both open and covert political, media and societal influence to promote Russian economic interests in the Czech Republic").

[152] Finkle, *supra* note 150. The IT security firm Crowdstrike believes the Russian government is behind the activities of this Russian group, called "Energetic Bear," because of technical indicators as well as the analysis of the targets chosen and the data stolen. *See* Eduard Kovacs, *Russia Accused of Conducting Global Cyber Espionage Campaign*, SOFTPEDIA (Jan. 22, 2014, 9:30 AM), http://news.softpedia.com/news/Russia-Accused-of-Conducting-Global-Cyber-Espionage-Campaign-419457.shtml.

[153] COUNTERINTELLIGENCE REPORT, *supra* note 8, at 1. *See also* Jason Ryan, *FBI Director Says Cyberthreat Will Surpass Threat from Terrorists*, ABC NEWS (Jan. 31, 2012), http://abcnews.go.com/blogs/politics/2012/01/fbi-director-says-cyberthreat-will-surpass-threat-from-terrorists.).

[154] COUNTERINTELLIGENCE REPORT, *supra* note 8, at 1.

[155] COUNTERINTELLIGENCE REPORT, *supra* note 8, at 1. In October 2007, Russian President Vladimir Putin asked the new head of Russia's external intelligence service, Sluzhba Vnehny Razvedi (SVR), former Prime Minister Mikhail Fradkov

Despite the fact that cyberattacks from Russia are a distant second to those from China,[156] there have been a significant amount of reports about the damage done by Russian malware. Hackers based in Russia gained access to computers in NATO, Western European governments, Ukrainian government organizations, energy and telecommunications companies in Europe, and U.S. academic institutions by utilizing a flaw in Microsoft Windows between 2009 and 2014.[157] The vulnerability, dubbed "SandWorm," was found in the OLE (Object Linking and Embedding) package manager in Microsoft Windows and Server.[158] In this case, "malicious Microsoft PowerPoint files would make the OLE packager download additional malicious files that allowed the attackers to execute commands on the targeted systems."[159] The SandWorm hackers had "been operating for at least five years and had been targeting institutions and individuals considered to work for Russian interests."[160]

Russian government hackers were suspected in 2014 of creating malware named "Uroburos" which could "move across machines even if they were not connected to the public Internet" and were designed to steal files from nation states' infrastructure, intelligence agencies, and high profile enterprises.[161] "The Russian connection was made after researchers from G-Data discovered plenty of Russian language strings in the code."[162] "They also found the malware was searching for the presence of Agent.BTZ,[163] malware used in

---

to build up the SVR's economic espionage capabilities. Christopher Burgess, *Nation States' Espionage and Counterespionage*, CSO (Feb. 13, 2008, 7:00 AM), http://www.csoonline.com/article/2122400/employee-protection/nation-states--espionage-and-counterespionage.html.

156 Burgess, *supra* note 155.

157 *Russia used Windows flaw to spy for years: Researchers*, PHYSORG (Oct. 14, 2014), http://phys.org/news/2014-10-russia-windows-flaw-spy-years.html.

158 Zeljka Zorz, *Russian Espionage Group Used Windows 0-Day to Target NATO*, NET SECURITY (Oct. 14, 2014), http://www.net-security.org/secworld.php?id=17491.

159 *Id*.

160 *Id. See generally Briefings – August 5–6,* BLACK HAT, https://www.blackhat.com/us-15/briefings.html.

161 Brewster, *supra* note 15.

162 Brewster, *supra* note 15.

163 Agent.BTZ was used in a massive cyber espionage operation on U.S. Central command that surfaced in 2008 and is one of the most serious U.S. breaches to date. Brewster, *supra* note 15.

attacks on the U.S. in 2008, which were said to have been carried out by Russian spies." "The Agent.BTZ attack was initiated when a USB stick was deliberately left in a parking area belonging to the United States Department of Defense" for an unwitting employee to discover and use.[164]

Others have been troubled not by Russian hackers, but by the rise of the Russian-based Kaspersky Lab. Kaspersky Lab sells anti-virus and internet security software to millions of people worldwide with Microsoft, Cisco, and Juniper Networks all embedding Kaspersky code into their products.[165] Each time a user downloads an application onto their desktop, data is sent to the company's Moscow headquarters.[166] Eugene Kaspersky, its CEO, is one of Russia's richest men and was KGB-trained, used to be a Soviet intelligence officer, and is currently aligned with Vladimir Putin's regime and Russia's Federal Security Service.[167]

According to its "State Armament Plan 2011–2020," the Russian government decided to reorganize and modernize its entire military and has already tripled its defense budget to the equivalent of just over $700 billion U.S. Dollars.[168] "As a result of Russia's modernization initiative, government-funded entities are increasing their footprint in the United States by seeking joint ventures with U.S. companies and academic institutions that possess sensitive R&D facilities, dual-use (commercial and military) technologies, sensitive proprietary information and classified technologies . . . saving the Russian government millions of R&D dollars."[169]

---

[164] Brewster, *supra* note 15.

[165] Noah Shachtman, *Russia's Top Cyber Sleuth Foils U.S. Spies, Helps Kremlin Pals*, WIRED (July 23, 2012, 4:00 AM), http://www.wired.com/2012/07/ff_kaspersky/all. Eugene Kaspersky has 300 million customers. His geek squad uncovers U.S. cyberweapons like stuxnet and flame. And he has deep ties to the KGB in Moscow. *Id*. *See also Eugene Kaspersky Chairman and CEO of Kaspersky Lab*, KASPERSKY LAB, http://usa.kaspersky.com/eugene-kaspersky.

[166] Shachtman, *supra* note 165.

[167] *Id.*

[168] Franz-Stefan Gady, *Russia's Military Spending to Increase Modestly in 2016*, THE DIPLOMAT (Nov. 10, 2015), http://thediplomat.com/2015/11/russias-military-spending-to-increase-modestly-in-2016/.

[169] *Joint Venture- an Opportunity to Lose*, COUNTERINTELLIGENCE STRATEGIC PARTNERSHIP NEWSLETTER (FBI, Washington, D.C.), Oct. 2013 at 6.

In June 2010, eleven SVR officers were arrested for illegally exporting high-tech microelectronics from the United States to Russian military and intelligence agencies.[170] "The microelectronics allegedly exported to Russia are subject to strict government controls due to their potential use in a wide range of military systems, including radar and surveillance systems, [weapons] guidance systems, and detonation triggers."[171] Alexander Fishenko, founder and CEO of Arc Electronics, Inc., a company claiming to produce technology for traffic lights and navigation systems, "was also charged with operating as an unregistered agent of the Russian government inside the United States by illegally procuring the high-tech microelectronics on behalf of the Russian government."[172]

"In the Soviet Union there was no statutory form of trade secrets protection."[173] However, the Russian Criminal Code was amended in 2014 to grant such protection.

### C. *France*

France is one country that seems to be at peace with the idea that nations can be economic competitors in the global marketplace even if politically aligned on other interests.[174] Industry and government are intricately intertwined in France. During a German television interview, France's former General Directorate for External Security (DGSE),[175] Director Claude Silberzahn, admitted publicly that for "decades" France has engaged in economic spying on behalf of

---

[170] The indictments were against a Russian agent and 10 other members of procurement network for Russia military and intelligence, operating in the United States and Russia. Designated by the Department of Commerce, defendants also included Texas and Russia based corporations. The Department of Commerce also designated 165 foreign persons and companies who received, transshipped, or otherwise facilitated the export of controlled commodities by the defendants to its "Entity List." Press Release, U.S. Dep't of Justice, Fed. Bureau of Investigation, Russian Agent and 10 Other Members of Procurement Network for Russian Military and Intelligence Operating in the U.S. and Russia Indicted in New York (Oct. 3, 2012) [hereinafter Russian Indictment Press Release].

[171] *Id.*

[172] *Id*.

[173] *See* LIMPERT & IATSYK, *supra* note 78 § 2-3(d)(i).

[174] HEDIEH NAHERI, ECONOMIC ESPIONAGE AND INDUSTRIAL SPYING 13 (Cambridge Univ. Press 2005).

[175] The DGSE is France's external intelligence agency.

state-owned industries.[176] He stated that in France, "the state is not just responsible for lawmaking, it is in business as well."[177] "It has been widely reported that France, for example, routinely bugged Air France flights and French hotel rooms to obtain economic and technical information from selected foreign passengers and guests."[178] Pierre Marion, another former DGSE Director, also admitted in a 1991 NBC news interview that he implemented an economic espionage campaign targeting American companies in the early 80s.[179]

"France is the Empire of Evil in terms of technology theft, and Germany knows it," said Berry Smutny, head of German satellite company OHIB Technology, in a 2009 diplomatic cable.[180] The communique, leaked in 2011, discussed rival contracts for a satellite navigation system. Smutny was suspended after the cable became public.[181]

Currently, Art. 418 of the French Criminal Code prohibits the theft of manufacturing secrets,[182] and "[l]ike Swiss and German law, French law recognizes a specific crime for the communication of trade secrets to foreigners or abroad."[183] France has proposed new legislation or changes to its existing laws in order to help mitigate

---

[176] F. W. RUSTMANN, JR., CIA, INC.: ECONOMIC ESPIONAGE AND THE CRAFT OF BUSINESS INTELLIGENCE (2002).

[177] "As former French intelligence chief Pierre Marion pointed out, 'it is an elementary blunder to think we're allies. When it comes to business, it's war.'" NASHERI, *supra* note 174.

[178] CHARLES MITCHELL, A SHORT COURSE IN INTERNATIONAL BUSINESS ETHICS 128 (World Trade Press, 3rd ed. 2009).

[179] *French Have Been Spying on U.S. Businesses, NBC Says*, DESERET NEWS (Sept. 14 1991 12:00 AM), http://www.deseretnews.com/article/182953/FRENCH-HAVE-BEEN-SPYING-ON-US-BUSINESSES-NBC-SAYS.html?pg=all.

[180] Adam Piore, *The Secret War*, Popular Mechanics, Feb. 2012 at 21, 23; Joshua Norman, *WikiLeaks: France Leads Russia, China in Industrial Spying in Europe*, CBS NEWS (Jan. 4, 2011), http://www.cbsnews.com/news/wikileaks-france-leads-russia-china-in-industrial-spying-in-europe/.

[181] Piore, *supra* note 180, at 23.

[182] A manufacturing secret is "a manufacturing process which has a practical or commercial interest and which the manufacturer keeps hidden from its competitors." *See* LIMPERT & IATSYK, *supra* note 78 § 2.3(c)(iv).

[183] *Id*.

the effects of economic espionage.[184] "France is also considering a public economic intelligence policy and a classification system for business information."[185] "France created a 12-person Economic Intelligence Office in 2009 to coordinate French corporate intelligence efforts."[186]

### D. *India*

India suffers from incredibly lax laws on spying and intellectual property theft. According to one report, "private detective agencies [in India] receive more than 10 requests a day by companies to spy on their rivals."[187] A survey by KPMG showed that 14 percent of Indian companies have been victims of corporate spying, with many companies not willing to admit intellectual property had been stolen.[188]

Cyberattacks coming out of India appear to be a new hybrid of sorts because Indian hackers are taking some of their cues from Chinese hackers. For the last few years, a diverse cyberespionage campaign has grown out of India that has targeted a variety of industrial entities around the globe, mainly Pakistan and U.S. organizations as well as the Norwegian telecom provider, Telenor, and the Chicago Mercantile Exchange.[189] Researchers from Norman Security reported on "the so-called Operation Hangover campaign that security

---

[184] TRADE SECRETS, *supra* note 1 at B-3; GIBSON DUNN & CRUTCHER LLP, 2014 YEAR-END FRENCH LAW UPDATE 11 (2014), http://www.gibsondunn.com/publications/Documents/2014-Year-End-French-Law-Update.pdf.

[185] TRADE SECRETS, *supra* note 1 at B-3.

[186] TRADE SECRETS, *supra* note 1 at B-3.

[187] *Corporate Spying a Booming Business in India*, REDIFF (May 17, 2011), http://www.rediff.com/business/slide-show/slide-show-1-corporate-spying-a-booming-business-in-india/20110517.htm.

[188] Jason Overdorf, *Industrial Espionage Booming in Corporate India*, GLOBALPOST: MONEY (Jan. 2, 2011), http://www.globalpost.com/dispatch/india/101223/industrial-espionage-corporate-india.

[189] Kelly Jackson Higgins, *'Commercialized' Cyberespionage Attacks Out of India Targeting United States, Pakistan, China, And Others*, DARK READING (May 20, 2013, 2:47 PM), http://www.darkreading.com/attacks-breaches/commercialized-cyberespionage-attacks-ou/240155245; Alex Cox, *Don't Fear the Hangover – Network Detection of Hangover Malware Samples,* RSA – SPEAKING OF SECURITY (May 20, 2013), https://blogs.rsa.com/dont-fear-the-hangover-network-detection-of-hangover-malware-samples/..

experts say appears to be run by an independent cyberespionage organization-for-hire organization and demonstrates the vast and potentially lucrative nature of cyberspying in the global market."[190]

"The group behind Operation Hangover appears to represent a new advanced persistent threat (APT) model" and "possibly implicates a commercial Indian security firm", thus Indian government-sponsorship has not been confirmed.[191] "Unlike the constant and ubiquitous wave of cyberespionage attacks against U.S. interests by China, Operation Hangover has more global and for-hire characteristics," which makes it more difficult to determine "whether the operation is a nation-state endeavor."[192]

### E. *Israel*

A recently revealed NSA document, among many disclosed by former NSA contractor Edward Snowden, shows Israel to be a valued and trusted military ally, but also a country that spies on the U.S. and targets U.S. technology.[193] The NSA document quoted from a 2013 National Intelligence Estimate on cyber threats which "ranked Israel the third most aggressive intelligence service against the U.S." behind only China and Russia.[194] Two reports by Newsweek, published in May 2014, on Israeli spying also alleged that the extent of Israeli espionage activities in the U.S. was "sobering" and "shocking."[195] According to a 2005 FBI report, Israel has an active program

---

[190] Higgins, *supra* note 189.

[191] *Id.*

[192] Higgins, *supra* note 189. "Hangover appears to be a more 'standardized' or franchised operation, with freelancers writing code and regular patterns of establishing domains and placing images on them." Snorre Fagerland, the principal security researcher in the malware detection team at Norman Security's Shark team says, "[i]t's like one of the call centers of the APT . . . There are indications to some extent that the attack may be contracted—it might be a service provided to somebody.'" *Id.*

[193] Jeff Stein, *Israel Flagged as Top Spy Threat to U.S. in New Snowden/NSA Document*, NEWSWEEK (Aug. 4, 2014, 2:16 PM), http://www.newsweek.com/israel-flagged-top-spy-threat-us-new-snowdennsa-document-262991. *See also* GLENN GREENWALD, NO PLACE TO HIDE (2014).

[194] Stein, *supra* note 193.

[195] Times of Israel Staff, *New NSA Document Highlights Israel's Espionage in the U.S.*, TIMES OF ISRAEL (May 17, 2014, 8:38 PM), http://www.timesofisrael.com/new-nsa-document-highlights-israeli-espionage-in-us/.

to gather information from within the U.S., which includes recruitment of spies and computer intrusion.[196] "These collection activities are primarily directed at obtaining information on military systems and advanced computing applications that can benefit Israel's armaments industry."[197] One way Israel recruits spies is by encouraging Israeli representatives and businessmen to attend conferences and defense contracting facilities.[198] The idea is to entice American scientists to visit Israel in order to obtain U.S. military and civilian technologies.[199]

One such American scientist, Stewart David Nozette, worked at the White House on the National Space Council before being convicted in 2011 for spying for Israel.[200] Nozette is speculated to have been compensated at least $225,000 for handing over classified information to Israel.[201] The Office of Naval Investigations later learned that Israel sold these U.S. trade secrets to other countries.[202] One such trade secret was Phalcon, an early warning aircraft based on U.S. licensed technology, which Israel attempted to sell to China in 2000.[203] Israel also "sold advanced weapons systems to China that incorporated technology developed by American companies—including the Python-3 air-to-air missile and Delilah cruise missile. There is evidence that Israel stole Patriot missile avionics to incorporate into its Arrow system and that it used US technology obtained

---

196 Philip Giraldi, Questioning Military Aid to Israel, Press Briefing sponsored by the Council for the National Interest (June 8, 2011) (transcript available at http://ariwatch.com/OurAlly/IsraeliMilitaryAndIndustrialEspionage.htm).

197 *Id.* at 2.

198 Jeff Stein, *Israel's Aggressive Spying in the U.S. Mostly Hushed Up*, NEWSWEEK (May 8, 2014, 10:50 AM), http://www.newsweek.com/israels-aggressive-spying-us-mostly-hushed-250278.

199 *Id*.

200 Giraldi, *supra* note 196, at 3.

201 Giraldi, *supra* note 196, at 3.

202 OFFICE OF THE NAT'L COUNTERINTELLIGENCE EXEC., NCIX 2006-009, ANNUAL REPORT TO CONGRESS ON FOREIGN ECONOMIC COLLECTION AND INDUSTRIAL ESPIONAGE (2005).

203 Wade Boese, *Israel Halts Chinese Phalcon Deal*, ARMS CONTROL ASSOCIATION (Sept. 1, 2000), https://www.armscontrol.org/act/2000_09/israelsept00.

in its Lavi fighter development program—which cost the US taxpayer about $1.5 billion—to help the Chinese develop their J-10 fighter."[204]

The recruitment of U.S. citizens for Israel's spy service does not end with scientists. Pentagon intelligence analyst, Lawrence Franklin, gave classified materials to an Israeli Embassy intelligence officer, as well as American Israel Public Affairs Committee (AIPAC) officials, and is consequently serving a twelve-year prison sentence.[205] Israel also sent citizens posing as art students to U.S. military bases with the intention of gaining physical entry to government offices, residences of government employees, and Defense Department facilities.[206] Many of these "students" were found entering federal buildings from back doors and parking garages, and most of the students had backgrounds in "military intelligence, electronic surveillance intercept, or explosive ordinance units."[207]

## IV. AN EVALUATION OF THE GLOBAL RESPONSE TO ECONOMIC ESPIONAGE

### A. *Why the U.S. response has been weak*

There are several reasons why the U.S. approach to combatting economic espionage is weak: (1) the criminal statute, 18 U.S.C. § 1831, has requirements that are difficult to prove, (2) the sentences under § 1831 are minimal, (3) despite being educated on the pitfalls of lax cybersecurity and personnel controls, there is a lack of buy-in from private industry to cooperate with law enforcement and/or tighten office security measures to prevent IP theft, (4) the federal government has taken a relatively hands-off approach in assisting private enterprise, and (5) other countries do not assist in international investigations due to their own weak response or individual

---

[204] Giraldi, *supra* note 196, at 1.

[205] David Johnston, *Pentagon Analyst Gets 12 Years for Disclosing Data*, N. Y. TIMES (Jan. 20, 2006), http://www.nytimes.com/2006/01/20/politics/20cndfranklin.html?_r=0.

[206] Christopher Ketcham, *The Israeli "Art Student" Mystery*, SALON (May 7, 2002, 3:12 PM), http://www.salon.com/2002/05/07/students/.

[207] Philip Giraldi, *The Spy Who Loves Us*, INFORMATION CLEARING HOUSE, (Oct. 6, 2008), http://www.informationclearinghouse.info/article20065.htm.

attitudes towards intellectual property theft or in some cases, are the same foreign countries involved in the theft.

### 1. THE WEAKNESSES IN 18 U.S.C. § 1831

There are several reasons why there have been few economic espionage convictions under § 1831, one being the statute itself. The EEA contains a difficult element to prove, that is, the foreign government/agent/instrumentality nexus requirement. The government must prove that the defendant knew or intended that his actions would benefit a foreign government, instrumentality, or agent.[208] As Thomas Reilly, a trial attorney in the Counterespionage Section of the National Security Division writes,

> The purpose behind the expansion of the intended beneficiaries beyond foreign governments and foreign agents is to preclude evasion of the statute by foreign governments hiding behind corporate or other shell entities. An analysis of proof regarding a foreign instrumentality requires a lot of investigation into the structure, function, operation, personnel, and conduct of the instrumentality and its business and relationship with the foreign government . . . This evidence comes in many forms, primarily from a defendant's own statements and documents, a money trail, public records, a mutual legal assistance treaty, letters rogatory, evidentiary requests, and expert witnesses who can explain the relationship among foreign entities and how the foreign government can benefit from the offense.[209]

Proving government sponsorship is particularly difficult when states "build relationships with hackers to develop customized malware or remote-access exploits to steal sensitive US economic or technology information, just as certain FIS (foreign intelligence services) have already done."[210] "FIS and other foreign entities have

---

[208] 18 U.S.C. § 1831(a) (2012).

[209] Thomas Reilly, *Economic Espionage Charges Under Title 18 U.S.C. 1831: Getting Charges Approved and the "Foreign Instrumentality" Element*, 57 U.S. ATT'YS BULL. 24 (2009).

[210] COUNTERINTELLIGENCE REPORT, *supra* note 8, at ii.

used independent hackers at times to augment their capabilities and act as proxies for intrusions, thereby providing plausible deniability."[211] Oftentimes, cybersecurity firms can determine the source of the hack from the IP range and the particular language of the hacker code. Chinese attacks are known to be constant and persistent, and they come from several hackers in one giant, steady stream rather than from one hacker, making it difficult to determine if the attack is government sponsored.

Proof of government sponsorship in the case of China is easier to find than with many other countries that attempt to install layers of protection between those stealing the secrets and any government entity.[212] The central government in China has been linked to many Chinese commercial entities, and those entities have been "affiliated with PLA ["the People's Liberation Army"] research institutes or have ties to and are subject to the control of government organizations such as the State-Owned Assets Supervision and Administration Commission."[213]

A common defense to economic espionage and theft of trade secrets is to attack the statutory requirement that the information stolen was, in fact, a "trade secret," one which the owner took reasonable measures to keep the information secret and one that has independent economic value.[214] If the defendant can prove that the information was in the public domain or dispute the ownership of the information, the defendant may not be convicted.[215]

Another common defense is for the defendant to allege reverse engineering, which means that the beneficiary did not receive stolen trade secrets, but rather others were able to conduct research and analyze the product or information and determine how it worked or

---

[211] COUNTERINTELLIGENCE REPORT, *supra* note 8, at 1.

[212] ANNUAL REPORT TO CONGRESS 2014, *supra* note 125, at 13 ("China has used its intelligence services and other illicit approaches to collect sensitive U.S. information and export- controlled technology in violation of U.S. laws and export controls" to gain access to information they cannot access under the guise of civilian enterprise).

[213] *Id.*

[214] 18 U.S.C. § 1839(3)(A) (2012); 18 U.S.C. § 1839(3)(B) (2012).

[215] Thomas Dougherty, *Common Defenses in Theft of Trade Secret Cases*, 57 U.S. ATT'YS BULL. 27, 31 (2009).

how it was made or manufactured *on their own*.[216] In these situations, the government must attempt to show that "the defendant obtained the trade secret information without the authorization of the trade secret owner."[217]

The defense most commonly used is the "tool kit" defense, in which the government fails to prove that the defendant intended to share proprietary information with someone *other than* the owner of the trade secrets.[218] The defendant alleges that he/she merely wanted to download information at work for their own personal knowledge for future personal use.[219] This defense goes to the heart of a necessary element of prosecution that the defendant intended to convert the trade secrets to the economic benefit of someone other than the owner. It is difficult to prove this element if the defendant downloaded his or her own work so that he/she could use the non-confidential information in the future, and confidential information was inadvertently transferred along with non-confidential information.[220]

The U.S. government has made some improvements to the statute since the EEA was passed in 1996 to make it easier to prosecute these cases. Initially, federal prosecutors working under a U.S. Attorney would first seek approval to open an EEA investigation from the Assistant Attorney General for the National Security Division of the Department of Justice before charging anyone with economic espionage.[221] Recently, authorization to initiate EEA cases has been

---

[216] *Id.* (citing Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 476 (1974) and ConFold Pac., Inc. v. Polaris Indus., 433 F.3d 952 (7th Cir. 2006)).

[217] *Id*. at 32.

[218] *See id.* at 27 (citing theft of trade secrets case, United States v. Shiah, No. SA CR 06-92, 2008 U.S. Dist. LEXIS 11973 (C.D. Cal. Feb. 19, 2008)).

[219] *See id.* at 28 (illustrating a case where "[t]he court found that the defendant's actions were consistent with his explanation that he compiled a "tool kit" of information in downloading the body of his work at his place of employment so that he could use the nonconfidential information in the future").

[220] Dougherty, *supra* note 215, at 28 (illustrating a case where the government failed to prove the defendant downloaded the content for use of the confidential information because the defendant testified that he only intended to use the non-confidential information and downloaded the confidential information inadvertently).

[221] Reilly, *supra* note 209, at 24. Until 2011, 28 C.F.R. § 0.64-5 (2015) set forth the requirement that the Attorney General, Deputy General, Assistant Attorney General for National Security, or the Assistant Attorney General, Criminal

streamlined. It is unclear whether the decrease in red tape will have a significant impact in the rise or decline of open economic espionage cases. Several suggestions to improve the ease of prosecution under the EEA have arisen to include enacting a companion federal civil cause of action,[222] proposing both civil and criminal penalties for the failure to report the theft and establishing a whistleblower defense to encourage parties to report suspected thefts,[223] focusing on corporate accountability and employee awareness rather than prosecution,[224] and more carefully calibrating the EEA to the important societal IP interests at stake.[225]

### 2. LACK OF PUNISHMENT UNDER 1831

Federal judges have been less than uniform in their opinions and views on economic espionage, theft of trade secrets, and the penalties that should be meted out for those offenses. One judge sent a definitive message to China by giving one Chinese spy, Greg Chung, nearly 16 years' imprisonment and exclaimed at the sentencing, "[s]top sending your spies here."[226] In another theft of trade secret case in Tennessee, the district court felt the circumstances did not warrant incarceration and gave both defendants four months' home confinement and a $1,000 fine.[227]

---

Division must provide personal approval in order for the United States to file a charge under EEA.

[222] Kelley Clements Keller & Brian M.Z. Reece, *Economic Espionage and Theft of Trade Secrets: The Case for a Federal Cause of Action*, 16 TUL. J. TECH. & INTELL. PROP. 1, 3–4 (2013).

[223] David Orozco, *Amending the Economic Espionage Act to Require the Disclosure of National Security-Related Technology Thefts*, 62 CATH. U.L. REV. 877, 881–82 (2013).

[224] Brittani N. Baldwin, *Keeping Secrets: An Alternative to the Economic Espionage Penalty enhancement Act*, 32 TEMP. J. SCI. TECH. & ENVTL. L. 45, 46 (2013).

[225] Adam Cohen, *Securing Trade Secrets in the Information Age: Upgrading the Economic Espionage Act After* United States v. Aleynikov, 30 YALE J. ON REG. 189, 191–92 (2013).

[226] Judge Carney at the sentencing hearing of Greg Chung on Feb. 8, 2010 where Chung was sentence to 188 months imprisonment. Press Release, U.S. Attorney's Office, Cent. Dist. of Cal. Release No. 10-027, Former Boeing Engineer Sentenced to Nearly 16 Years in Prison for Stealing Aerospace Secrets for China (Feb. 8, 2010).

[227] In late 2011, the company announced that MESNAC Co. of China was taking a 100 percent equity position. Bill Brewer, *Wyko Tire Technology Sold to*

Federal judges have shown a distinct bias in handing out minimal sentences for economic espionage or intellectual property theft compared to cases dealing with "typical" espionage, i.e., theft of unclassified intellectual property versus classified information. The penalty for espionage can be death or life in prison,[228] whereas economic espionage and theft of trade secrets provide maximum penalties of 15 and 10 years respectively.[229] Spies who steal classified secrets frequently receive maximum sentences under the guidelines, whereas spies who steal trade secrets receive light sentences under the guidelines, typically a few years or substantially less. The table below reflects the disparity in sentencing in cases involving spies who steal classified information working on behalf of a foreign power, compared to the light sentences handed out to defendants in cases dealing with theft of trade secrets.[230] Either federal judges are unaware of the dire ramifications of economic espionage to national security, or they believe theft of trade secrets is less heinous and more defensible than traditional espionage.

---

*China Co.*, KNOXVILLE NEW SENTINEL (Dec. 1, 2011, 8:00 PM), http://www.knoxnews.com/business/wyko-tire-technology-sold-to-china-company. Clark Roberts and Sean Howley were arrested March 6, 2009. Press Release, U.S. Dep't of Justice, Office of Public Affairs, Two Indicted for Conspiring to Steal Trade Secrets from Goodyear Tire and Rubber Company (Mar. 6, 2009). They were both convicted on December 9 2010 for one count of conspiracy to commit trade secret theft, one count of trade secret theft, one count of unlawful photographing of trade secrets, three counts of transmittal of trade secrets, one count of possession of trade secrets, two counts of wire fraud and one count of conspiracy to commit wire fraud. Press Release, U.S. Dep't of Justice, Office of Public Affairs, Two Engineers Found Guilty of Stealing Goodyear Trade Secrets (Dec. 9, 2010). The District Court sentenced both men to four years probation, four months home confinement, and 150 hours of community service. *See* United States v. Howley, 707 F.3d 575, 579 (6th Cir. 2013). On June 3, 2013, Howley and Roberts were resentenced to four years probation and 150 hours of community service. Both men, who were originally sentenced in 2011, have already completed community service. Howley and Roberts also served four months home confinement as part of their original sentence, and paid a $1,000 penalty.

228 18 U.S.C. § 794 (2012).

229 18 U.S.C. §§ 1831, 1832 (2012).

230 *See* table for comparison.

| Year | Spy | Country | Secret | Sentence |
|---|---|---|---|---|
| 1977 | Christopher John Boyce & Andrew Daulton Lee | USSR | Highly sensitive data relating to U.S. satellite systems | Boyce: 40 years imprisonment; Lee: life imprisonment |
| 1978 | William Peter Kampiles | USSR | Technical manual relating to one of America's most important spy satellites | 40 years imprisonment |
| 1980 | Henry David Barnett, CIA employee | USSR | Became a mole at the behest of the KGB; sold CIA secrets | 18 years imprisonment |
| 1981 | Joseph George Helmich | USSR | Information relating to a "Top Secret" U.S. communications system | Life imprisonment |
| 1981 | William Holden Bell | USSR | Large amount of military related technology | 8 years imprisonment |
| 1985 | Jonathan Jay Pollard | Israel; China | | Life imprisonment |
| 1994 | Aldrich Ames, CIA Counterintelligence Chief | USSR | Spied for nine years and handed over comprehensive blueprints of U.S. collection operations against the Russians including the identities of undercover agents | Life imprisonment |
| 2001 | Robert Hanssen, FBI special agent | USSR | Over 6,000 pages of classified documents on sensitive national security programs, including the details of U.S. nuclear war defenses. Also revealed the identities of Russian agents working for the United States | Life imprisonment |
| 2001 | Ana Belen Montes, Senior Analyst for DIA | Cuba | | 25 years imprisonment[231] |

[231] The information in this table is from DEF. PERSONNEL SECURITY RES. CENTER, ESPIONAGE AND OTHER COMPROMISES OF NATIONAL SECURITY: CASE SUMMARIES FROM 1975 TO 2008 (2009), https://fas.org/irp/eprint/esp-summ.pdf.

The bias and contrast between how federal judges sentence those who steal classified information versus unclassified trade secrets is similar to the disparity and contrast between the sentences handed out for cases involving violent criminals versus white collar crime offenders.

According to the United States Sentencing Commission, the average prison sentence length (not actual time served) every year from 1991 to 2001 for white-collar and corporate criminals was between 19.0 and 20.8 months. During the same period, however, violent offenders' and drug offenders' sentences ranged from 89.5 to 106.7 months and 71.7 to 88.2 months, respectively. Often, white-collar criminals have been given lighter sentences than petty robbers.[232]

When comparing economic espionage sentences to federal violent crime sentences, we also see a trend towards harshly penalizing offenders of violent crimes much more than economic spies. Perhaps this is because economic espionage tends to look more like a white collar crime and white collar crime is treated more softly than violent crime.[233]

### 3. PRIVATE INDUSTRY INDIFFERENCE

One of the main reasons why there are so few economic espionage convictions in the U.S. is the lack of buy-in from the private sector. Currently, companies are not legally required to report a loss of sensitive information or a remote computer intrusion to the

---

[232] J. Scott Dutcher, *From the Boardroom to the Cellblock: The Justifications for Harsher Punishment of White-Collar and Corporate Crime*, 37 ARIZ. ST. L.J. 1300, 1301–02 (2005) ("While the robber with the fountain pen often causes much more economic harm than the man with the six-gun, the fountain-pen robber has traditionally been treated less harshly. Historically, white-collar crime in the United States has been punished very lightly in comparison to violent crimes where the victim is physically injured or put at risk to be physically injured. "In the federal system, the argument that white-collar offenders receive shorter sentences than street criminals who commit proportional crimes has strong empirical backing").

[233] Elizabeth Szockyj, *Imprisoning White-Collar Criminals?*, 23 S. ILL. U. L.J. 485, at 487–88 (1998-1999) ("One study, which examined violations by Fortune 500 corporations over a two-year period, found that corporate executives were convicted in only 1.5% of all enforcement actions").

FBI.[234] Private companies fear the disclosure that their trade secrets have been stolen may impact their shareholders' and the public's view of the health and stability of the company due to the theft. How will the theft impact the stock price? Announcing a security breach of this nature could tarnish a company's reputation and endanger its relationships with investors, bankers, suppliers, customers, and other stakeholders.

The result is few companies disclose the theft. "Google announced in 2010 that China-based hackers had raided its networks," and stolen its source code.[235] At the same time, at least thirty-four other companies were also victims of the same cyberattack, but only two, Intel and Adobe Systems, Inc. admitted to being hacked.[236]

Companies also fear that the trade secret may be disclosed in court, thus further devaluing their work. This fear is unfounded since the EEA contains a special provision in section 1835 to protect against the disclosure of specific trade secret information throughout criminal proceedings, which includes discovery, pre-trial, and trial proceedings.[237] The judge issues a protective order precluding either side from mentioning trade secret specifics.[238]

Another reason for the lack of prosecutions lies in the fact that oftentimes, it can take a company years to learn the technology was

---

[234] The Defense Security Service currently requires cleared defense contractors to report any IP theft to the FBI. *Targeting U.S. Technologies: A Trend Analysis of Cleared Industry Reporting*, DEFENSE SECURITY SERVICE 10 (2013), http://www.dss.mil/documents/ci/2013%20Unclass%20Targeting%20US%20Technologies_FINAL.pdf

[235] Riley & Walcott, *supra* note 11.

[236] Riley & Walcott, *supra* note 11. "I can't find an organization, an entity, a business, or a department that hasn't suffered from cyber intrusions." Piore, *supra* note 11 (quoting Gordon M. Snow, assistant director of the FBI's Cyber Division) (internal quotations omitted).

[237] 18 U.S.C. § 1835 (2012).

[238] *Id.*

"In any prosecution or other proceeding under this chapter, the court shall enter such orders and take such other action as may be necessary and appropriate to preserve the confidentiality of trade secrets, consistent with the requirements of the Federal Rules of Criminal and Civil Procedure, the Federal Rules of Evidence, and all other applicable laws. An interlocutory appeal by the United States shall lie from a decision or order of a district court authorizing or directing the disclosure of any trade secret." *Id.*

stolen.[239] A company may only learn of the theft when a foreign competitor puts out the very same product at a significantly reduced price. The loss of this technology can come from a trusted insider or from a computer intrusion. According to Mandiant, an American cybersecurity firm, it takes an average of 229 days for organizations to discover their breach.[240] In 2013, only 33% of organizations self-detected a breach compared to 37% in 2012.[241]

American businessmen and women have also demonstrated a certain apathy towards economic espionage, almost arguing that, while it is unfair, it is inevitable. Perhaps the act of stealing trade secrets hits too close to home, e.g., the "tool kit" defense ("I'm collecting work information for my own future, personal use"), which seems reasonable and understandable. "A recent survey by the Ponemon Institute and Symantec showed that close to 60 percent of employees who have resigned or been terminated admit they stole company data."[242] And "less than 3 percent of all information technology and security dollars are spent to safeguard electronic or hard copy corporate information."[243] Moreover, if companies spent significant amounts of money on cybersecurity and the company is, in fact, never hacked or information never stolen, then business executives are left answering to shareholders as to why they spent so much money with no tangible benefit. This motivates executives to risk the cyber threat and spend the money on other business needs.

---

[239] Moreover, when companies identify the theft, "it is . . . difficult to assign an economic value to some types of stolen information . . . . [F]or example, it would be nearly impossible to estimate the monetary value of talking points for a meeting between officials from a [U.S.] company and foreign counterparts." COUNTERINTELLIGENCE REPORT, *supra* note 8, at 3.

[240] MANDIANT, 2014 THREAT REPORT: BEYOND THE BREACH 1 (2014).

[241] MANDIANT, *supra* note 240, at 1. "Previously 'the No. 1 priority was to protect the operational security of the investigation and the prosecutive equities on the criminal side.' While those goals are still important, 'it's even more important that the victims understand they have been victimized.'" Piore, *supra* note 11 (quoting Jonathan Pollet, the founder of Red Tiger Security in Houston).

[242] *Employers: Keep your trade secrets secret*, BUS. LEGAL RESOURCES (August 27, 2013), http://hr.blr.com/HR-news/Staffing-Training/Employment-Contracts/Employers-Keep-your-trade-secrets-secret. *See also Keep Your Secrets Locked Up Tight*, HR NEWS (Apr. 6, 2011), http://inshaiimtprofessionalcollege.blogspot.com/2011/04/keep-your-secrets-locked-up-tight.html.

[243] *Id*.

While some believe U.S. economic success hinges on innovation and new technology, along with certain proprietary protections provided to the innovators in compensation for the risks they take, others feel the U.S. is an open society and intellectual property should be shared with the world at large for the benefit of mankind. A case in point is that of J. Reece Roth, Professor Emeritus at the University of Tennessee in the Engineering Department and project manager, who was hired to develop plasma based aerodynamic controls for use in small unmanned aerial vehicles and guided munitions, and was convicted of violating the Arms Export Control Act in 2011.[244] Roth had hired a Chinese national and Iranian national as graduate students to work on a top secret military project after signing a contract specifically stating that no foreign persons were permitted to work on the project.[245]

Companies have always gathered their own intelligence—examples include looking at a competitor's prices, soliciting feedback from customers, conducting surveys or public views on competitor practices and product value, etc. While most business "executives would agree that protecting a company's confidential data and trade secrets from the prying eyes of competitors is critical,"one study of senior IT security executives "revealed that 65 percent [of executives] are aware that their company has experienced a computer intrusion in which data was stolen, and 55 percent have discovered a current employee or insider taking information from the company's computer system to use in a competing business."[246] This leads one to believe corporate theft may be prevalent, but apparently it is not enough of a concern to spend significant time and resources to fix the problem.

---

[244] Tom Chester, *Feds Investigating Retired UT Professor*, KNOXVILLE NEWS SENTINEL (July 11, 2006), http://www.knoxnews.com/news/local-news/feds-investigating-retired-ut-professor. *See generally* United States v. Roth, 628 F.3d 827 (6th Cir. 2011).

[245] United States v. Roth, 628 F.3d 827, 830 (6th Cir. 2011).

[246] *What Are The Top Security Concerns of Senior IT Executives?*, NET SECURITY (June 4, 2014), http://www.net-security.org/secworld.php?id=16955 [hereinafter *Top Security Concerns of Senior IT Executives*]. According to Gordon M. Snow, assistant director of the FBI's Cyber Division, "We have to have a cultural shift in the nation where we understand that there is no secure system, that people are going to be hacked." Piore, *supra* note 11.

There is a great likelihood that U.S. corporate executives, in particular, do not understand the full extent of existing cybersecurity risks or the employee insider threat. As to cybersecurity risks, a 2012 Carnegie Mellon University CyLab report revealed that

> corporate boards and executives are taking risk management seriously but there is still a gap in understanding the link between information technology (IT) risks and enterprise risk management. This gap indicates that boards have a lack of understanding of how all business operations are supported by computer systems and digital data and how risks in these areas can undermine operations. Less than two-thirds of the respondents' organizations have full-time personnel in key roles for privacy and security . . . [and] Asian boards (76 percent) are much more likely to have a board Risk Committee responsible for privacy and security than North American (40 percent) and European (38 percent) boards.[247]

---

[247] *Top Executives in Critical Infrastructure Cite Need for Improvement in Managing Cyber Risks*, EMC (May 16, 2012) [hereinafter *Top Executives*], http://www.emc.com/about/news/press/2012/20120516-01.htm. *See also* Jody R. Westby, *How Boards & Senior Executives Are Managing Cyber Risks*, CARNEGIE MELLON U. CYLAB 5–7, 24 (May 16, 2012), http://www.hsgac.senate.gov/imo/media/doc/CYBER%20Carneigie%20Mellon%20report.pdf; *Energy, Other Utilities' Cybersecurity is Weak*, U.S. SENATE'S HOMELAND SECURITY & GOVERNMENT AFFAIRS COMMITTEE (May 17, 2012) [hereinafter *Energy*], https://www.hsgac.senate.gov/media/majority-media/energy-other-utilities-cybersecurity-is-weak.According to the third biennial Carnegie Mellon University CyLab survey of boards of directors and senior management, "57 percent of energy and utility company executives said they rarely or never reviewed security program assessments. The energy sector and other utilities ranked lowest among industries in security management of their cyber assets." *Energy*, *supra*. "The U.S. generally believes it is the global leader in security, but the survey results indicate that North American boards lag behind European and Asian boards in undertaking key activities associated with privacy and security governance such as regular reviews involving annual budgets, roles and responsibilities, and top-level policies." *Top Executives*, *supra*.

As Richard Clarke once suggested, are U.S. businesses waiting for a "cyber Pearl Harbor"[248] to occur before addressing the problem?

### 4. THE WEAK RELATIONSHIP BETWEEN THE FEDERAL GOVERNMENT AND PRIVATE INDUSTRY

The United States has been labeled "hypocritical" in that the U.S. government has been accused of authorizing intelligence gathering against allies and enemies alike while at the same time Congress has made economic espionage illegal. This comment was especially made after Edward Snowden disclosed the depth of the National Security Agency's ("NSA") surveillance capabilities in June of 2013, and countries began to justify their own espionage activities by arguing "you do it too" and "we're just trying to keep up."[249] In fact, after the Snowden disclosures, experts in counterintelligence

---

[248] At a Milken Institute conference in 2014, Richard Clarke, CEO of Good Harbor Security Risk Management and a former U.S counterterrorism official, stated, "What companies have to realize is, while we're waiting for a cyber Pearl Harbor that may become a national problem, companies have a problem every day . . . What you're losing every day is intellectual property, research and development, and business intelligence, and you're losing money because they create accounts payable and send money offshore." Rick Newman, *China May Have Hacked Your Company, Too*, YAHOO FINANCE (May 20, 2014), http://finance.yahoo.com/blogs/daily-ticker/china-has-probably-hacked-your-company--too-175016269.html.

[249] China argues that the U.S. is the nation state leading the cyberwar, and it needs to do more to protect itself in the coming years. J. Nicholas Hoover, *NSA Chief: China Behind RSA Attacks*, DARK READING (Mar. 27, 2012, 3:12 PM), http://www.informationweek.com/news/government/security/232700341; *NSA Chief: Chinese Steal a "Great Deal" of Military-Related Intellectual Property, and Were Responsible for Last year's Attacks on Cybersecurity Company RSA*, INFORMATIONWEEK (Mar. 27, 2012); The Liberation Army Daily, an unofficial but well-vetted source, issued a report, which stated, "The U.S. military is hastening to seize the commanding military heights on the Internet, and another Internet war is being pushed to a stormy peak . . . .Their actions remind us that to protect the nation's Internet security, we must accelerate Internet defense development and accelerate steps to make a strong Internet army." Paul Rosenzweig, *Beware of Cyber China*, HOOVER INSTITUTION (March 15, 2012), http://www.hoover.org/research/beware-cyber-china.

reported "a fivefold increase in physical espionage attempts against U.S. businesses" and a threefold increase in cyberespionage.[250]

News articles such as those written by Glenn Greenwald, who interviewed Snowden in Hong Kong, certainly fanned the flames. In one article, Greenwald referenced an email written by an NSA spokesperson who claims "'[t]he department does ***not*** engage in economic espionage in any domain, including cyber,'" yet Greenwald pointed out that the NSA has been found to spy on "plainly financial targets such as the Brazilian oil giant Petrobas; economic summits; international credit card and banking systems; the EU antitrust commissioner investigating Google, Microsoft, and Intel; and the International Monetary Fund and World Bank."[251]

In response to the Petrobas spying allegations, Director of National Intelligence ("DNI") James Clapper stated, "It is not a secret that the Intelligence Community ("IC") collects information about economic and financial matters . . . .What we do not do, as we have said many times, is use our foreign intelligence capabilities to steal the trade secrets of foreign companies on behalf of—or give intelligence we collect to—U.S. companies to enhance their international competitiveness or increase their bottom line."[252]

---

[250] Joshua Philipp, *After Snowden, Global Espionage Increased Fivefold,* EPOCH TIMES (May 30, 2014), http://www.theepochtimes.com/n3/704132-after-snowden-global-espionage-increased-fivehold/?photo=4. According to Verizon's 2014 Data Breach Investigations Report, "[t]he United States was by far the largest target of cyberespionage, being hit with 87 percent of espionage incidents . . . .South Korea was second, being targeted by 6 percent of attacks." *Id.*

[251] Glenn Greenwald, *The U.S. Government's Secret Plans to Spy for American Corporations*, INTERCEPT, (Sept. 5, 2014), https://theintercept.com/2014/09/05/us-governments-plans-use-economic-espionage-benefit-american-corporations. *See also* GREENWALD, *supra* note 193, at 134–35. "Much of the Snowden archive revealed what can only be called economic espionage: eavesdropping and email interception aimed at the Brazilian oil giant Petrobras, economic conferences in Latin America, energy companies in Venezuela and Mexico, and spying by the NSA's allies—including Canada, Norway, and Sweden—on the Brazilian ministry of Mines and Energy and energy companies in several other countries." *Id.*

[252] Greenwald cites a DNI-sponsored 2009 Quadrennial Intelligence Community Review Final Report ("QICR") that appears to provide evidence, albeit inconclusive, that at a minimum the U.S. Intelligence Community has contingency plans to engage in economic espionage under certain scenarios that specifically threaten national security. GREENWALD, *supra* note 193, at 135. *See also* OFFICE OF THE DIR. NAT'L INTELLIGENCE, QUADRENNIAL INTELLIGENCE

Obviously, the U.S. cannot make economic espionage illegal, admonish other countries for engaging in these practices, and then do the same in secret. After an exhaustive search looking for evidence that the U.S. government passes on pilfered economic intelligence to aid domestic private business, one can only find allegations of collection, but not evidence of an actual transfer of secrets to private enterprise.[253] Even Glenn Greenwald admits in his book *No*

---

COMMUNITY REVIEW: FINAL REPORT APRIL 2009 (2009) [hereinafter FINAL REPORT 2009], https://pdf.yt/d/NKHjTMZwaSYhg1KP. The report described how "experts from across the [IC], other U.S. departments and agencies, academia, think tanks, and industry assessed the implications of the year 2025 for the IC." *Id.* at i. "QICR 2009 developed alternative future scenarios based on *Global Trends 2025* to explore concepts and capabilities the IC may need to fulfill critical missions in support of U.S. national security." *Id.* However, "[i]t d[id] not purport that any one future will materialize, but rather outlined a range of plausible futures so that the IC could best posture itself to meet the range of challenges it may face." *Id.*

In response to Greenwald's inquiries about QICR 2009 and future plans for U.S. government-sponsored industrial espionage—which was contemplated under one dire scenario—U.S. officials continue to insist that using surveillance capabilities to bestow economic advantage for the benefit of a country's corporations is wrong, immoral, and illegal. Yet according to Greenwald, this 2009 report advocates doing exactly that in the event "that the technological capacity of foreign multinational corporations could outstrip that of U.S. corporations." GREENWALD, *supra* note 193 (internal quotations omitted). Using covert cyber operations to pilfer "proprietary information" and then determining how it "would be useful to U.S. industry" is precisely what the U.S. government has been vehemently insisting it does not do, even though for years it has officially prepared to do precisely that. *Id.*

[253] "[F]ormer U.S. officials insist the government does not engage in economic espionage or intellectual property theft from foreign companies. In part, they contend that's because there is little IP we would want to steal, and to do so would undercut our efforts to discourage such theft by other nations. Private U.S. companies, meanwhile, would be breaking U.S. law if they hacked into the servers of state-owned competitors in places like China and Russia." Piore, *supra* note 11. Joel Brenner, former head of U.S. counterintelligence during the Bush and Obama administrations, has said, "The U.S. has an enormous stake in the integrity of the intellectual property regime . . . Many of our adversaries don't believe we don't do this. But it's really true. We don't." *Id*. (internal quotations omitted). "[T]his apparent unwillingness to retaliate presents an 'asymmetric disadvantage' that our rivals are exploiting to win an emerging digital cold war." *Id*. (quoting a digital security expert at the Washington D.C.-based Center for Strategic and International Studies). "The New York Times noted that its surveillance targets often included financial institutions and 'heads of international aid organizations,

*Place to Hide* that the National Security Agency ("NSA") "acts for the benefit of what it calls its 'customers,' a list that includes not only the White House, the State Department, and the CIA, but also primarily economic agencies such as the US Trade Representative and the Department of Agriculture, Treasury, and Commerce."[254]

Espionage is a reality. All countries conduct espionage, and their main intention is to collect data.[255] This data is collected so governments may learn of the intentions, capabilities, and motivations of other nation states. It would be extremely helpful for any government official to learn the strategies of foreign competitors before trade and economic talks just as it is important to learn the military battle plans of adversaries before an actual engagement of hostilities.[256]

---

foreign energy companies and a European Union official involved in antitrust battles with American technology businesses . . . .' U.S. and British agencies 'monitored the communications of senior European Union officials, foreign leaders including African heads of state, directors of United Nation and other relief programs [such as UNICEF], and officials overseeing oil and finance ministries . . . .' When the United States uses the NSA to eavesdrop on the planning strategies of other countries during trade and economic talks, it can gain enormous advantage for American industry." GREENWALD, *supra* note 193, at 138.

[254] GREENWALD, *supra* note 193, at 135–36.

[255] "Allies often suspect each other of economic espionage—underlining how countries can be partners in traditional security matters yet competitors in business and trade . . . . According to a 2010 press report, the Germans view France and the United States as the primary perpetrators of economic espionage 'among friends.' France's Central Directorate for Domestic Intelligence has called China and the United States the leading 'hackers' of French businesses, according to a 2011 press report." COUNTERINTELLIGENCE REPORT, *supra* note 8, at B–2.

[256] Hillary Clinton is quoted as saying: "When I would go to China or I would go to Russia . . . we would leave all my electronic equipment on the plane with the batteries out, because this is a new frontier and they're trying to find out not just about what we do in our government, they're trying to find out about what a lot of companies do and they were going after the personal emails of people who worked in the State Department. It's not like the only government in the world that is doing anything is the United States." Daily Mail Reporter, *'His Leaks Helped Terrorists': Hillary Clinton Blasts NSA Leaker Edward Snowden*, DAILY MAIL (last updated Apr. 26, 2014, 8:52 AM) (internal quotations omitted), http://www.dailymail.co.uk/news/article-2613670/His-leaks-helped-terrorists-Hillary-Clinton-blasts-NSA-leaker-Edward-Snowden.html?ITO=1490&ns_mchannel=rss&ns_campaign=1490.

What distinguishes the United States from, say, China, is that the U.S. does not steal economic intelligence or foreign proprietary corporate information to benefit American private industry. In countries such as China, France, Israel, and Russia, where industry is promoted by its government and private business has extensive ties to the government, there is a strong possibility that any economic and trade intelligence collected may be shared with private or state-owned businesses in those countries to one degree or another.

The United States government has been given the authority to undertake economic espionage under the inherent executive powers assigned to the President within Article II of the U.S. Constitution. Article II provides that all executive powers shall be vested in the President of the United States, and one aspect of this power is the authority to conduct espionage for purposes of national security, e.g., General Washington authorized the use of spies during the Revolutionary War.[257] Typically, this has involved political espionage rather than economic espionage. The federal courts, though, have not drawn a line segregating one from the other and have been loath to limit the President's use of executive authority when dealing with foreign nations and international disputes.[258]

With such authority provided, why then has economic espionage been abjured by the United States when our allies and competitors do it all the time? There are several reasons, including the concept of federalism, which creates a distance between the federal government and private industry; the U.S. political culture; and the First Amendment, which keeps our capitalist economy open for all and allows for uninhibited lobbying by domestic and international companies.

The U.S. government, rooted in federalism principles, is prohibited from acting on behalf of U.S. companies. The national government is one of limited and enumerated powers, with states retaining

---

[257] Madalyn Velie, *Espionage Tactics*, GEORGE WASHINGTON'S MOUNT VERNON, http://www.mountvernon.org/digital-encyclopedia/article/espionage-tactics/ (last visited Apr. 18, 2016) (discussing President George Washington's use of spies).

[258] *See* the Chaco Border Dispute that was the basis for *United States v. Curtiss-Wright Export Corp.*, 299 U.S. 304, 3330–31 (1936), and *see* the Iran hostage crisis that was the basis for *Dames & Moore v. Regan*, 453 U.S. 654, 662–66, 278–79 (1981).

residual powers such as registering companies.[259] Unlike unitary states like the UK or France where companies register with and are licensed by the central government, in the U.S., this is done at the state level and therefore the connection between companies and the federal government is much weaker. Moreover, states are prohibited from favoring an in-state company over an out-of-state competitor. Under the dormant or negative commerce clause, the Supreme Court has prohibited state governments from imposing impediments to foreign and out of state commerce, e.g., states cannot favor a local dairy or agrarian interest over an out-of-state rival.[260]

Second, the United States, more than others, is premised on a free market ideology that corresponds with a limited national government. The U.S. government and U.S. political culture see the optimal outcome resulting from a free market allocation of resources and have chosen, unlike France or China, to not pick "national winners" in industry. Most American government officials do not believe economic espionage will enrich the nation, but will, most likely lead to retaliatory measures taken against American companies and individuals, which would be harmful because the U.S. remains the world's superpower with the largest economy in the world.

The United States, as the largest developed economy in the world, promotes an open and fair trading system to engender economic growth, democracy and international stability; the government remains focused on international trade rules, which, other things being equal, create the most favorable outcome for American industry and workers. As such, the U.S. has sought to lead by example and perhaps downplay the occasional loss of intellectual property when allies take advantage of our openness.

Lastly, the United States is part of a global economy where large multi-national corporations employ tens of thousands of people in dozens of countries worldwide. It would be difficult for the U.S. to steal trade secrets from one foreign corporation which perhaps employs thousands of American workers, share the pilfered intellectual property with a U.S.-based company in the same industry, and know

---

[259] Article I, Section 8, enumerated those limited powers, such as regulating interstate commerce, taxing and spending, but not the residual power to assist local companies. U.S. Const. art. I, § 8.

[260] Baldwin v. G.A.F. Seelig Inc., 294 U.S. 511, 522–22 (1935).

with any certainty these actions would not negatively impact the U.S.-based employees of that foreign entity. It is no longer clear who actually benefits and who is harmed from economic espionage in an interconnected global economy. It is possible to help one American company only to injure another. For example, imagine if the U.S. undertook espionage on behalf of General Motors or Chrysler against Volkswagen or Toyota. Although this might seem like a benefit to executives and employees at American car companies located in the industrial northeast and Midwest, it would be harmful to other Americans, such as workers in Tennessee and Kentucky where Volkswagen and Toyota have a large presence.

Thus, the U.S. system of federalism, capitalism, and individualism, and the fact that the U.S. sees itself as protector of the world's open trading system, best explains why economic espionage is not supported or tolerated by the U.S. government except in its current limited role, in that some economic intelligence is collected for national security purposes.

### 5. WHY THE GLOBAL RESPONSE HAS BEEN WEAK

"There's no country where we have a no-spy agreement."
—President Barack Obama[261]

Espionage is a dirty business. Spies act outside international, traditional norms in comparison to military maneuvers, which, for the most part, follow established international rules. A soldier is given the courtesy of POW status when engaging in combat and conducting operations in accordance with the laws and customs of war. A

---

[261] Zeke J. Miller, *Obama: "There's No Country Where We Have a No-Spy Agreement"*, TIME (Feb. 11, 2014) (This was President Obama's response when asked at a joint press conference with French President Francois Hollande "whether his choice of France for the first state visit of the second term indicated a new special relationship that would result in an extension of a so-called 'no-spy' agreement with the European ally."), http://time.com/6398/obama-theres-no-country-where-we-have-a-no-spy-agreement. Hollande responded by saying "he and Obama had put the controversy behind them, but said there must be an expectation of privacy for ordinary people around the world. 'Following the revelations that appeared due to Snowden, we clarified things, Mr. Obama and myself, we clarified things. And then this was in the past,' Hollande said 'Mutual trust has been restored.'" *Id.*

spy, when caught, is usually criminally prosecuted or held without POW status.

There is a general distaste for espionage. But economic espionage seems to engender a less visceral emotion, and governments are more forgiving in cases of intellectual property theft compared to the typical political and military espionage of the Cold War era. While political and military espionage seems to bring out aggressive, nationalistic tendencies to the forefront, economic espionage seems to be tied to a nation's economic survival, and therefore, deemed more "acceptable."

There are several factors that might influence a particular government to either support or reject the idea of state-sponsored economic espionage. The biggest factor, of course, is money and prosperity for one's people. Historically, as trends go, developing countries

> manufacture[] lower-technology products and provide[] lower-technology services for sale to the more developed countries. The developed countries, meanwhile, close[] entire industries and convert[] their labor forces to work on more advanced products and services based on newly invented products and processes. Prosperity increase[s] as new technologies dr[i]ve productivity gains and wages r[i]se. [Several] [c]ountries [have] moved up the technology ladder.[262]

However, moving up the technology ladder has become a much quicker proposition for some, especially if the trade secrets of one's competitors can be legally or illegally acquired, and so the concept of economic espionage is born.[263]

Developed countries with advanced intellectual property (IP) want to protect, benefit and promote their competitive advantage, so these countries enact laws to safeguard IP and reward entrepreneurs for sweat equity and taking risks. These laws are necessary, since "illegal theft of intellectual property . . . undermine[s] both the

---

[262] NAT'L BUREAU OF ASIAN RESEARCH, THE IP COMMISSION REPORT 9 (2013).

[263] *See generally id.*

means and the incentive for entrepreneurs to innovate, which[, [in turn,] slow[s] development of new inventions" and scientific discoveries.[264] On the other hand, developing countries have no incentive to protect what they do not have, and in an effort to catch up and become competitive themselves and bring economic prosperity to their people, those with a perceived need have little incentive to play by the same rules.[265]

Governments that are heavily intertwined with private industry are more likely to conduct economic espionage for the benefit of the private sector. Countries that have a nationalistic view of the "global" marketplace, and represent a target-rich environment of advanced technology for their competitors, tend to have strict IP protection laws and economic espionage-type criminal statutes. However, other countries that are just as nationalistic from an economic perspective, but have minimal protectionist industrial policies and poor legal environments for IP protection, may be among the countries that either support or condone economic espionage. Developed countries that have more to lose from the theft of their trade secrets and who value innovation (such as the United States) obviously favor enforcing and prosecuting economic crimes.

However, some developed countries, such as Canada and New Zealand, countries that have EEA-type legal protections in place, have not prosecuted anyone for such crimes; this perhaps may suggest that at least some in those governments believe that such prosecutions actually inhibit innovation and productivity rather than protect it. Then there is the perspective of many in countries such as China, Russia, and perhaps India, where intellectual property theft seems to be justified since it ensures a level playing field amongst developed and developing countries.[266]

In short order, economic espionage begins to look less like a moral judgment and more like a different perspective on the rule of law. While the U.S. is quick to label other governments as thieves, other countries may not consider what they are doing as wrong. Why is this so? While the U.S. capitalist system seeks to strongly protect property interests, other cultures seem to view intellectual property

---

[264] *Id.* at 1.

[265] *See id.* at 10.

[266] THE COMM'N ON THE THEFT OF AM. INTELLECTUAL PROP., THE IP COMMISSION REPORT (2013).

through a different lens and are less willing to declare IP a uniquely protected right.

Different conceptions of ownership and types of political governance may shape each country's unique view of the rule of law. The U.S. does not have public ownership of private property, whereas China has a history of common ownership of property. Similarly, the U.S. does not have the collusion between government and business like the state-owned industries in France or the possible collusion between the oligarchs and the Russian government.

The concept of individualism may also explain why the U.S. is the only nation to have utilized its economic espionage laws to prosecute offenders, whereas countries like Germany and Canada, which are more social welfare states, have not. The United States may have the strongest protections in the world, but in other countries such as Germany, while there is no specific economic espionage statute, trade and business secrets are protected albeit in less specific legal provisions.

The U.S. (and the Western world for the most part) tends to cherish individualism ("Be yourself! Set your own standard! Just say no!"),[267] whereas China and the East tend to value harmony and group solidarity ("Fit in with the others! Don't stick out! Find a way to say yes!").[268] These priorities in values demonstrate that China would be more willing to condone stealing trade secrets for the benefit of state-owned industry than a country such as the U.S., which emphasizes fair competition, individual ingenuity, and innovation.

Lastly, another reason why the global response to IP theft and economic espionage has been so weak is because historically, many nations have condoned these activities, including ironically in earlier years the United States. In the 19th century, the United States was known for stealing from the British, particularly in the textile industry.[269] American citizen, Francis Cabot Lowell, moved to Scotland in 1811 and secretly stole the plans to the Cartwright loom, a

---

[267] T.R. REID, CONFUCIUS LIVES NEXT DOOR: WHAT LIVING IN THE EAST TEACHES US ABOUT LIVING IN THE WEST 152 (Vintage Books 1999). T.R. Reid was the Washington Post Tokyo Bureau Chief and lived in Japan for five years.

[268] *Id.*

[269] *See* JOHN J. FIALKA, WAR BY OTHER MEANS: ECONOMIC ESPIONAGE IN AMERICA xi–xiv (W.W. Norton & Company, Inc. 1997).

water-driven weaving machine that almost singlehandedly had provided Britain with a booming economy.[270] Lowell then moved back to Boston, built a version of the Cartwright loom, and founded a town (Lowell) that "provided the first big shock that jolted America into the industrial age."[271]

Centuries earlier, the British did the same to the Chinese. The British, known for their love of tea, had a plant, camellia sinensis,[272] smuggled out of China and into India.[273] In 1848, Robert Fortune, working for the East India Company (with ties to the British government),

> 'learned Mandarin, shaved his head, adopted a pigtail as worn by Manchus, dressed in local clothes and disguised himself as a Chinese from a distant province. He sneaked into remote areas of Fujian and Jiangsu province, forbidden parts of China. Fortune managed to collect 20,000 plants and seedlings and had then transported it to Kolkata [(India)] in Wardian cases, small greenhouses which kept the plants healthy due to condensation within the case . . . .' These seedlings were planted in Darjeeling and grew into bushes that over the time produced the unique tea . . . .'[T]he knowledge that he brought back from China together with plants were instrumental in what is today a huge flourishing tea industry in India.'[274]

Now, with the Chinese stealing trade secrets from U.S. business entities, we have come full circle, since centuries earlier Chinese discoveries and technology were pilfered by the West. Some Chinese believe history justifies their current behavior, especially in

---

[270] *Id*. at xi–xiii.

[271] *Id*. at xiv.

[272] "Camellia Sinensis is the Latin word for tea." Subhro Niyogi, *Spy Secret Behind Darjeeling Tea*, TIMES INDIA (Feb. 7, 2014), http://timesofindia.indiatimes.com/city/kolkata/Spy-secret-behind-Darjeeling-tea/articleshow/29966599.cms.

[273] *Id.*

[274] *Id.*

view of "The Century of Humiliation," referring to the West's exploitation of China since the mid-19th century.[275] China was exploited and humiliated for over 100 years by an international system that strengthened their competitors and kept China weak, isolated, and divided. So China and its business community believe they have a right to do whatever they can get away with to assume their rightful place in the world. Some countries see no contradiction or harm in stealing the intellectual property of other nations. After all, is it not true that everything is fair in love, war and business?

Self-justification and feelings about the theft of trade secrets vary. The severity of the problem is certainly underestimated. Some nations and its citizens find theft of trade secrets from foreign competitors acceptable and deemed critical to the stability of their nation's economy; others find it unacceptable and blatantly illegal. Some countries will take extreme measures to improve or ensure the survival of their respective economies, even to include the outright theft of trade secrets. Regardless of one's particular view on the issue, the global response to economic espionage has been weak and ineffectual.

## V. CONCLUSION

In the United States, theft of trade secrets is illegal.[276] Competitive intelligence, also known as open-source intelligence, is perfectly legal. Every intelligence agency collects sensitive foreign political, military, technical and economic information. This intelligence is provided to government leaders to aid them in making policy decisions. In the case of economic and technical information, e.g., trade secrets, some foreign governments share that intelligence with domestic and state-owned industry providing those companies with a distinct unfair advantage over their foreign competitors. This is theft of intellectual property, the protection of which is a cornerstone of capitalism and free enterprise. The U.S. government denies stealing foreign trade secrets or intellectual property for the benefit

---

[275] *See* Helen H. Wang, 'Century of Humiliation' Complicates U.S.-China Relationship, FORBES, (Sept. 17, 2015) http://www.forbes.com/sites/helenwang/2015/09/17/century-of-humiliation-complicates-us-china-relationship/.

[276] See 18 U.S.C. §§ 1831, 1832 (2012).

of U.S. private industry; however, the U.S. Intelligence Community ("USIC") readily admits acquiring foreign economic intelligence for legitimate government purposes.

In 1996, when former President Bill Clinton signed the Economic Espionage Act, the U.S. government identified somewhere between 23 and 51 foreign nations, which were targeting sensitive U.S. technologies through human espionage and other means.[277] Since then, the USIC's annual assessment of countries spying on the U.S. has climbed consistently to well over 100 foreign countries including both adversaries and allies.[278] Countries now view national power and national security in economic terms, and the key to U.S. wealth and economic well being is our trade secrets. Since the U.S. is the most technologically advanced country, there is no doubt that its intellectual property is being targeted by multiple state-and-private actors.

> BlackOps Partners Corporation, which does counter-intelligence and protection of trade secrets and competitive advantage for Fortune 500 companies, estimates that $500 billion in raw innovation is stolen from U.S. companies each year. Raw innovation includes trade secrets, research and development, and products that give companies a competitive advantage. 'When this innovation is meant to drive revenue, profit, and jobs for at least 10 years, we are losing the equivalent of $5 trillion out of the U.S. economy every year to economic espionage,' said Casey Fleming, CEO of BlackOps Partners Corporation.[279]

---

[277] *See* H. R. REP. NO. 104-788, at 12-13 (1996); *see also* S. REP. NO. 104-359, at 6 (1996).

[278] Olga Khazan, *Actually, Most Countries Are Increasingly Spying on Their Citizens, the UN Says*, THE ATLANTIC (June 6, 2013), http://www.theatlantic.com/international/archive/2013/06/actually-most-countries-are-increasingly-spying-on-their-citizens-the-un-says/276614/; *see also* Michael Martinez, *Allies Spy On Allies Because a Friend Today May Not Be One Tomorrow*, CNN (Oct. 31, 2013), http://www.cnn.com/2013/10/30/us/spying-on-allies-everybody-does-it/.

[279] Joshua Philipp, *The Staggering Cost of Economic Espionage Against the U.S.*, EPOCH TIMES (last updated 1:13 PM), http://www.theepochtimes.com/n3/326002-the-staggering-cost-of-economic-espionage-against-the-us.

If the gross domestic product for the U.S. was $16.7 trillion dollars in 2013[280] with approximately 116 million full-time workers, how many additional U.S. jobs would have been created with an additional $5 trillion dollars of GDP? Economic espionage is obviously a major concern.

Unfortunately, the U.S. response to economic espionage has been relatively weak due to only a few actual convictions; poor reporting by the U.S. business community due to its fear of disclosure and damage to its reputation; private industries' lax cybersecurity and poor security against insider employee theft; and U.S. private sector apathy, or at best, feelings of inevitability that loss of trade secrets is merely a cost of doing business.

While the U.S. values innovation and spends billions[281] on R&D, the U.S. will more than likely not follow the example of China and Russia, or even France for that matter, where government and business interests are intricately entwined. The U.S. government structure is such that there will always be a separation between government and private industry and its citizens value their privacy sufficiently that corporations would be reluctant to become intimate partners with government agencies. What could change this dynamic? Economic espionage and the wholesale loss of U.S. intellectual property for one thing. If economic espionage goes unchecked in America, this could kill American innovation and the incentive to invest in technology, and ultimately lead to the Orwellian predictions discussed in Global Trends 2030, a futuristic study conducted by the Office of the Director of National Intelligence. "In 2030, Asia will have surpassed North America and Europe combined in terms of global power . . . .China's GDP . . . is likely be about 140-percent larger than Japan's."[282] "A reinvigorated US economy"—spurred by

---

[280] *GDP*, WORLD BANK (Nov. 29, 2015), http://data.worldbank.org/indicator/NY.GDP.MKTP.CD.

[281] "For 2008, the most recent year available, the NSF [("National Science Foundation")] calculated that U.S. industry, the Federal Government, universities, and other nonprofit organizations expended $398 billion on R&D, or 2.8 percent of the US Gross Domestic Product." COUNTERINTELLIGENCE REPORT, *supra* note 8, at 4.

[282] NAT'L INTELLIGENCE COUNCIL, GLOBAL TRENDS 2030: ALTERNATIVE WORLDS iv, 16 (2012), http://www.dni.gov/index.php/about/organization/global-trends-2030.

possible US energy dependence—"would increase the prospects that the growing global and regional challenges would be addressed."[283] If the US fails to rebound, "[a] dangerous global power vacuum would be created."[284]

U.S. businesses need to become educated, aware, and more proactive. Economic espionage and cyberattacks are not going away, in fact, it is getting worse.[285] Criminal prosecutions and sanctions should increase at a bare minimum, as this will send a strong message to other countries engaged in state-sponsored theft of trade secrets.

---

[283] *Id.* at 106.

[284] *Id.* "[I]t took Britain 155 years to double GDP per capita, with about 9 million people . . . The US and Germany took between 30 and 60 years with a few tens of million people . . . but India and China are doing this at a scale and pace not seen below: 100 times the people than Britain and a tenth the time. By 2030 Asia will be well on its way to returning to being the world's powerhouse, just as it was before 1500." *Id*. at 2.

[285] "The absence of universally accepted and enforceable norms of behavior in cyberspace has contributed to this situation . . . The result is a cyber environment in which multiple actors continue to test their adversaries' technical capabilities, political resolve, and thresholds." *Worldwide Threat Assessment of the U.S. Intelligence Community: Hearing Before Senate Armed Services Comm.*, 114th Cong. 2 (2015) (statement for the record of James R. Clapper, Director of National Intelligence), http://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf. In a Cisco Systems study, the number of devices such as smartphones and laptops in operation worldwide that can connect to the Internet and other networks is expected to increase from about 12.5 billion in 2010 to 25 billion in 2015. DAVE EVANS, THE INTERNET OF THINGS: HOW THE NEXT EVOLUTION OF THE INTERNET IS CHANGING EVERYTHING 3 (Cisco Internet Business Solutions Group 2011), http://www.iotsworldcongress.com/documents/4643185/3e968a44-2d12-4b73-9691-17ec508ff67b. There is an increase in cloud computing, and this movement of data among multiple locations creates vulnerabilities. With the globalization of the supply chain, we have become increasingly interconnected. Theft of trade secrets will happen more often with "the proliferation of smartphones and the inclination of employees to plug their personal devices into workplace networks and cart proprietary information around." Nicole Perlroth, *Traveling Light in a Time of Digital Thievery*, NEW YORK TIMES (Feb. 10, 2012), http://www.nytimes.com/2012/02/11/technology/electronic-security-a-worry-in-an-age-of-digital-espionage.html?_r=0.

However, an increase in Department of Justice and FBI resources to investigate and prosecute cases of trade-secret theft, especially by cyber means, plus enhanced outreach efforts to educate the private sector, will be insufficient to blunt the problem of IP theft and economic espionage. These efforts are merely putting a band-aid on an open artery. It is only until the theft becomes personal that businesses, employees, and the government will pay attention and take it seriously. A more holistic view and overreaching strategy is necessary,[286] and an understanding of how other nations perceive this problem and how they confront it may also prove to be beneficial. The lack of universally acceptable and enforceable norms have clearly undermined U.S. attempts to protect trade secrets. It is time for the global community, not just the United States, to re-evaluate these incredibly damaging activities and take drastic action to enact sufficient penalties and sanctions to blunt this economic and national security problem.

---

[286] Though outside the scope of this article, a starting point to redirect focus would be to limit access to the American market for those foreign companies identified as benefiting from competitive advantage through the fruits of trade secret theft. The U.S. must change the cost-benefit calculus for foreign entities that steal intellectual property. "Stealing American IP needs to have serious consequences, with costs sufficiently high that state and corporate behavior and policies that support IP theft are fundamentally changed. Companies that seek competitive advantages within the American market by using stolen intellectual property must find their access to that market made more difficult or thwarted altogether until they stop stealing." *see* NAT'L BUREAU OF ASIAN RESEARCH, *supra* note 264, at 22. In addition, U.S. corporate tax rules should stop rewarding private sector CEO's who off-shore and out-source our manufacturing jobs and R&D to China, where in short order the technology is stolen and used to compete against their erstwhile American partners. For additional suggestions, *see id.* at 4–7.