The Report committee for Claire Marie Huitt

Certifies that this is the approved version of the following report:

Whose Threat is it Anyway?

Addressing Economic Espionage in Law, Policy, and Practice

SUPERVISING COMMITTEE:

Robert Chesney, Supervisor

Derek Jinks, Co-supervisor

Whose Threat is it Anyway?

Addressing Cyber Economic Espionage in Law, Policy, and Practice

by

Claire Marie Huitt

Report

Presented to the Faculty of the Graduate School

of the University of Texas at Austin

in Partial Fulfillment

of the Requirements

for the Degrees of

Masters of Global Policy Studies

and

Doctor of Jurisprudence

The University of Texas at Austin

May 2021

Whose Threat it is Anyway?

Addressing Economic Espionage in Law, Policy, and Practice

by

Claire Marie Huitt, MGPS, JD

The University of Texas at Austin 2021

SUPERVISORS: Robert Chesney & Derek Jinks

Cyber economic espionage is a threat to national security. But unlike typical national security threats, economic espionage is also–and perhaps most immediately–a threat to American businesses. The frontline against economic espionage is not made up of typical national security actors; the frontline is made up of American companies, big and small. And American companies stand to lose a great deal. This report surveys current approaches to the economic espionage threat in law, policy, and private sector practices. Adequately addressing the threat requires a robust response from both the U.S. government and U.S. businesses. The responses of both, at present, are insufficient.

TABLE OF CONTENTS

Economic espionage by foreign governments targeting U.S. industry and innovation is an issue of tremendous importance to our national security and is one the Committee has been examining for some time . . . . In 1992, then-Director of Central Intelligence [(DCI)] Robert M. Gates told the committee: ``We know that some foreign intelligence services have turned from politics to economics and that the United States is their prime target.'

–*Special Report of the Senate Select Committee on Intelligence January 4, 1995 to October 3, 1996*[1]

We don't want to sit back and discover, years and years after the fact, that while we have investigated every reported security breach, spies have stolen our secrets or cyber thieves have exploited our networks . . . . We may spend billions of dollars to develop a given weapons system, the effectiveness of which rests on essential technological, operational or design secrets that give U.S. advantage. If those essential secrets are stolen, both our investments and our advantage can be lost.

–National Counterintelligence Executive, Michelle Van Cleave, 2005[2]

"[E]veryone in the room knew that by then, China had already collected enough U.S. intellectual property to last it well into the next decade. Chinese hackers had taken everything from the designs for the next F-35 fighter jet to the Google code, the U.S. smart grid, and the formulas for Coca-Cola and Benjamin Moore paint."

–*Nicole Perlroth, This is How They Tell Me the World Ends: The Cyber-Weapons Arms Race, 2021*[3]

I. BACKGROUND

Cyber economic espionage is a threat to American national security. The U.S. government has recognized and talked about it as a national security threat since the early to mid-nineties. And in the near three decades that have passed since then-DCI Gates's statement cited above, the threat has grown exponentially. Unlike typical

[1] S. Rep. No. 105-1 [hereinafter SSCI Report 1996].
[2] Michelle Van Cleave, Nat'l Counterintelligence Executive, Remarks at the Conference on Counterintelligence for the 21st Century: The National Counterintelligence Strategy of the U.S. 4–6 (Mar. 4–5, 2005) https://fas.org/irp/news/2005/03/ncix030505.pdf.
[3] NICOLE PERLROTH, THIS IS HOW THEY TELL ME THE WORLD ENDS: THE CYBER-WEAPONS ARMS RACE 281 (Bloomsbury Publishing, 2021).

national security threats, economic espionage is also–and perhaps most immediately–a threat to American businesses. State-sponsored theft of intellectual property (IP) and other proprietary information is a threat to national security insofar as it threatens the United States' economic health and competitive advantage. But the frontline against economic espionage is not made up of typical national security actors; the frontline is made up of American companies, big and small. And American companies stand to lose a great deal. Department of Commerce estimates place the value-added of U.S. IP-intensive industries to the U.S. economy around $6.6 trillion as of 2014[4]; and that estimate showed a 30% increase from estimates in 2010 that placed value-added around $5.06 trillion.[5] That means that from 2010 to 2014, IP-intensive industries went from accounting for around 34.8% to 38.2% of annual U.S. gross domestic product (GDP).[6] It stands to reason that today, there is even more on the line.

While the United States has long recognized economic espionage as an international challenge, China's use of economic espionage is what has brought attention back to this topic in current national security discussions. The People's Republic of China (PRC) is a rather prolific user of economic espionage, and it has long targeted U.S. industry.[7] The IP Commission Report, published in 2013, found that China accounted for somewhere between 50% and 80% of economic espionage directed at the United States.[8] In 2015, President Barack Obama reached an agreement with

---

[4] ECONOMICS & STATISTICS ADMINISTRATION & U.S. PATENT AND TRADEMARK OFF., INTELLECTUAL PROPERTY AND THE U.S. ECONOMY: 2016 UPDATE 22 (2016) https://www.uspto.gov/sites/default/files/documents/IPandtheUSEconomySept2016.pdf.
[5] *Id.*
[6] *Id.*
[7] *See* SSCI Report 1996, *supra* note 1 (identifying among those countries extensively involved in economic espionage targeting the U.S. as of 1996).
[8] DENNIS C. BLAIR & JON M. HUNTSMAN, JR., THE IP COMMISSION REPORT: THE REPORT OF THE COMMISSION ON THE THEFT OF AMERICAN INTELLECTUAL PROPERTY 3 (2013) [hereinafter IPCR 2013].

President Xi Jinping that neither country would conduct or knowingly support cyber-enabled theft of intellectual property.[9] When announcing the agreement, Obama stated– "we'll work together, and with other nations, to promote international rules of the road for appropriate conduct in cyberspace."[10] And for a period of about eighteen months, Chinese hacking subsided.[11] But, shortly after President Trump took office, as tensions relating to trade, technology-acquisition, and other issues between the U.S. and China rose, Chinese hacking resumed with force.[12]

In recent years, China has accelerated its use of economic espionage; it has focused, acutely on America's commercial and industrial prowess and on technologies that could give China a military advantage.[13] The 2021 Annual Threat Assessment of the U.S. Intelligence Community asserts that "China will remain the top threat to U.S. technological competitiveness as the [Chinese Communist Party (CCP)] targets key technology sectors and proprietary commercial and military technology from U.S. and allied companies and research institutions associated with defense, energy, finance,

[9] THE WHITE HOUSE OFF. OF THE PRESS SECRETARY, FACT SHEET: PRESIDENT XI JINPING'S STATE VISIT THE UNITED STATES (2015) [hereinafter Obama-Xi Agreement 2015], https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states .
[10] President Barack Obama, Remarks by President Obama and President Xi of the People's Republic of China in Joint Press Conference (Sep. 25, 2015) [hereinafter Joint Statement 2015], https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/remarks-president-obama-and-president-xi-peoples-republic-china-joint.
[11] David E. Sanger & Steven Lee Myers, *After a Hiatus, China Accelerates Cyberspying Efforts to Obtain U.S. Technology*, N.Y. TIMES (Nov. 29, 2018), https://www.nytimes.com/2018/11/29/us/politics/china-trump-cyberespionage.html.
[12] *Id.*
[13] *Id.*

and other sectors."[14] China's use of economic espionage to target these industries gives rise to legitimate national security concerns.[15]

But while China might be the adversary of the moment, China is far from being the only state to engage in economic espionage. This is a long-standing, international problem. Many states, including U.S. allies, have relied on economic espionage to collect and disseminate proprietary information from U.S. firms for economic gain.[16] A 1997 report from the Senate Select Committee on Intelligence (SSCI) identified France and Israel–alongside China, Russia, Iran, and Cuba–as being "*extensively* engaged in economic espionage" against U.S. firms.[17] Worries about economic espionage by these countries in the nineties brought about a number of annual reports,[18] all of which concluded that "countries assessed to be actively collecting against U.S. interests have shown particular determination, and in most cases a willingness to use illegal and covert means, to collect U.S. economic and technological information."[19] Reports found that foreign collection focused primarily on science and technology information and products across a variety of industries including aerospace, biotechnology, chemical and biological systems, computer software and hardware, defense technology, energy

[14] OFF. OF THE DIRECTOR OF NATIONAL INTELLIGENCE, ANNUAL THREAT ASSESSMENT OF THE U.S. INTELLIGENCE COMMUNITY 7 (2021).
[15] It is important to point out that in recent years, worries about Chinese economic espionage have also been used to advance harmful anti-China sentiments in the US. Muddling the security threat posed by economic espionage with racially and politically motivated speech and actions undermines a state's ability to effectively address the threat. For a robust discussion of how racial bias currently impacts U.S. economic espionage prosecutions, *see* Andrew Congseh Kim, *Prosecuting Chinese "Spies": An Empirical Analysis of the Economic Espionage Act*, 40 CARDOZO LAW REVIEW 751 (2018).
[16] Susan W. Brenner & Anthony C. Crescenzi, *State-Sponsored Crime: The Futility of the Economic Espionage Act*, 28 HOUS. J. INT'L L. 389, 399 (2006).
[17] S. Rep. No. 105-1, *supra* note 1 (1997) (emphasis added).
[18] *E.g.*, OFF. OF THE NAT'L COUNTERINTELLIGENCE EXECUTIVE, ANNUAL REPORT TO CONGRESS ON FOREIGN ECONOMIC COLLECTION AND INDUSTRIAL ESPIONAGE: 1996 (1996) [hereinafter ONCIX 1996 Report].
[19] *Id.* at 1.

research, information systems, manufacturing, nuclear systems, telecommunications, and many more.[20]

To address the problem, Congress enacted the Economic Espionage Act (EEA) in 1996 which specifically criminalized the theft of proprietary information carried out in connection with a foreign government.[21] The EEA remains one of the U.S. government's primary tools to address the threat. For the U.S. and a handful of other countries, criminalization has been a key component in a broader strategy of using indictments and–when possible–prosecutions to deter and disrupt economic espionage.[22] But for many years now, the efficacy of the EEA and the indictment strategy has been widely debated.[23]

II. OVERVIEW

Twenty-five years after the EEA's enactment, economic espionage is a far more prevalent problem, and it stands to do a great deal more damage to the U.S. economy. And the threat continues to evolve alongside technology. Economic espionage is now, very often, cyber economic espionage. The National Counterintelligence and Security Center reports that "foreign intelligence services–and threat actors working on their behalf continue to represent the most persistent and pervasive cyber intelligence threat," and China, Russia, and Iran "stand out as three of the most capable and active cyber actors tied to economic espionage and the potential theft of trade secrets and

[20] *Id.* at 7.
[21] 18 U.S.C. §1831-2 (1996).
[22] *See* Melanie Reid, *A Comparative Approach to Economic Espionage: Is Any Nation Effectively Dealing With This Global Threat?*, 70 U. MIAMI L. REV. 757 (2016) (discussing how different countries approach economic espionage).
[23] *E.g.* Garret Hinck & Tim Maurer, *What's the Point of Charging Foreign State-Linked Hackers?*, LAWFARE (May 24, 2019), https://www.lawfareblog.com/whats-point-charging-foreign-state-linked-hackers.

proprietary information."[24] Discussions about how to defend against economic espionage are, at least in part, discussions about cybersecurity. And while reacting to economic espionage is a responsibility largely left to the U.S. government, defending against economic espionage is a responsibility largely left to the private sector.

This report surveys current approaches to the economic espionage threat in law, policy, and private sector practices. Adequately addressing the threat requires a robust response from both the U.S. government and U.S. businesses. The responses of both, at present, are insufficient.

Part one of this report provides more substance about the threat itself. Part one is split into two sections: (A) defining the threat and (B) quantifying the threat. This report is about cyber-enabled economic espionage, and it is concerned, narrowly, with state-sponsored acts. To better define the threat that those acts pose, the first section asks four questions: (i) is economic espionage really a threat to national security? (ii) Is economic espionage any different from a state's other espionage activities? (iii) How do cyber capabilities change the threat? And (iv) how do different states approach the practice of economic espionage? The second section then attempts to quantify the impact of economic espionage. Estimates of the impact of economic espionage vary, but most put the cost in terms of hundreds of billions of dollars and millions of jobs, annually. However, underreporting and other data problems makes it very hard–if not impossible–to know the full scope and scale of the problem.

Part two surveys current responses to economic espionage in U.S. law and policy. As noted, the US has long used criminalization as its most prominent tool in

[24] NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER, FOREIGN ECONOMIC ESPIONAGE IN CYBERSPACE 5 (2018) [hereinafter NCSC 2018].

combating economic espionage. Therefore, much of this section is dedicated to discussing the efficacy of criminalization. But there are other legal and policy tools to evaluate as well. In U.S. law and policy civil enforcement, trade tariffs, and bilateral agreements all play important roles in the way the state currently responds to economic espionage. And those tools are just how a state may *react* to the problem; the other element to response is how states *defend* against the problem. The U.S. government protects its own networks and provides a number of opportunities for public/private partnership, information sharing, and cybersecurity and information security education or training–all of which are designed to encourage the private sector to do a better job preventing theft. But the U.S. approach to improving private sector defense is very much dependent on the private sector's voluntary participation. Other countries have taken a regulatory approach to the problem–in some cases mandating private industry compliance with security standards or reporting requirements.

Despite current efforts to either defend against or respond to the problem, economic espionage persists. It continues to cost U.S. businesses and the U.S. economy hundreds of billions of dollars and millions of jobs each year. Part three discusses how the U.S. government and U.S. businesses can more effectively address the threat. There are a number of steps that can be taken to improve the US's reactive response–for example, improving incident reporting can help better illustrate the scale and scope of the problem. In turn, increasing reporting would help make enforcement efforts more effective. Which industries are suffering the most? How can law enforcement authorities and the Justice Department allocate their resources most efficiently?

But ultimately, reactive policies will always be insufficient on their own to address the threat. What is most critical now–what could do the most good in alleviating the cost of economic espionage–is improving defenses. There are a number of legislative or regulatory steps the U.S. government could take to incentivize or even require better private sector practices. Incentive programs in particular are an attractive way to increase private sector buy-in. But the private sector should also recognize that the bigger the problem becomes, the more likely statutory or regulatory intervention, mandating better defense becomes. If U.S. businesses what to avoid the specter of added government intervention–as they so often do–and stem the theft of their trade secrets, then it is in their best interest to strengthen their own defensive capabilities.

III. ARTICULATING THE THREAT

A. DEFINING ECONOMIC ESPIONAGE

Most simply put, economic espionage is a form of cheating; [25] think of it as looking off of the proprietary homework of a fellow nation-state. Acts of economic espionage may target a company's business strategies and plans, intellectual property, or research and development projects.[26] In doing so, the actor can erode the company's competitive economic advantage in the international marketplace, "placing the acquirer an unfair leap ahead on technological developments."[27]

[25] Reid, *supra* note 22, at 760.
[26] Catherine Lotrionte, *Countering State-Sponsored Cyber Economic Espionage Under International Law*, 40 N.C.J. Int'l L. & Com. Reg. 443, 452 (2015).
[27] *Id.*

In this report, economic espionage refers to *state*-sponsored theft of trade secrets and other proprietary information for economic gain. The formal definition provided by the FBI and adopted in this report is as follows:

> Economic espionage is foreign power-sponsored or coordinated intelligence activity directed at the U.S. government or U.S. corporations, establishments, or persons, designed to unlawfully or clandestinely influence sensitive economic policy decisions or to unlawfully obtain sensitive financial, trade, or economic policy information; proprietary economic information; or critical technologies. This theft, through open and clandestine methods, can provide foreign entities with vital proprietary economic information at a fraction of the true cost of its research and development, causing significant economic losses.[28]

Under this rather narrow definition, economic espionage is distinct from other kinds of IP and trade secret theft. It is common to hear terms like economic espionage, industrial espionage, corporate espionage, etc. used interchangeably, but here, we are not talking about one company spying on its market rival. For purposes of this analysis, we are talking, specifically, about acts carried out by or for a foreign government. A similar distinction is made in the EEA; under the statutory language, a person commits economic espionage when she knowingly engages in certain behavior either intending or knowing that it will benefit a foreign government, foreign instrumentality, or foreign agent.[29] What that phrase really entails is the subject of a much lengthier discussion below, but at this point in the analysis it is sufficient to say economic espionage is a state-sponsored activity.

The involvement of a foreign power changes the nature and severity of the threat. Hypothetically, if PepsiCo stole Coca-Cola's trade secrets, Coca-Cola would

[28] *What is "economic espionage"?*, DEP'T OF JUST. FED. BUREAU OF INVESTIGATION (last visited Feb. 6, 2021), https://www.fbi.gov/about/faqs/what-is-economic-espionage.
[29] 18 U.S.C. § 1831 (2012).

suffer financial losses, and there would be various avenues in U.S. law to hold PepsiCo and its agents liable in some form. But–though PepsiCo at one time may have wielded a nontrivial amount of military might[30]–this incident would likely not be considered a threat to U.S. national security. Nor would we expect this incident to have any impact on U.S. foreign relations. Somewhat less hypothetically,[31] the same cannot be said if China stole Coca-Cola's trade secrets. Coca-Cola would still suffer the financial losses, and there would be avenues in U.S. law to *try* to hold individual actors liable in some form. Though, when the actors are foreign nationals, it can be far harder (and often impossible) to get them into a U.S. courtroom. The incident will negatively impact US-China relations. We are talking trade secrets relating to soda, so the national security consequences of this incident may seem fairly remote. But it is important to remember that this is not a singular or isolated incident. Proprietary information is stolen from U.S. businesses every day. That impacts revenue, jobs, and ultimately, the U.S. economy. And additionally, not all targeted trade secrets relate to soda.

---

[30] *See* Flora Lewis, "Soviets Buy American," NEW YORK TIMES (May 10, 1989) (discussing a business deal in which PepsiCo purchased a number of warships and submarines from the Soviets as a form of 'payment' for opening new Pepsi plants in the Soviet Union), https://www.nytimes.com/1989/05/10/opinion/foreign-affairs-soviets-buy-american.html.

[31] On April 22, 2021, Dr. Xiaorong "Shannon" You, a U.S. citizen, was convicted on multiple charges, including economic espionage, for stealing Coca-Cola's trade secrets for the benefit of the Chinese government. The trade secrets related to the chemical formula used to coat cans of Coca-Cola, and the value of the trade secrets has been evaluated at approximately $120 million. At trial it was shown that You stole these trade secrets while employed by Coca-Cola in order to establish a can-coating manufacturing company in China in partnership with an existing Chinese chemical company. You received millions of dollars in funding from the Chinese government–in part from the Thousand Talent Program–to support the new manufacturing venture. In a number of similar cases, the Justice Department has been able to show that China's Thousand Talent Program and other programs like it are used to solicit and reward theft of American trade secrets. You was not the only person indicted in relation to this incident; Liu Xiangchen, a Chinese national was also indicted as a coconspirator. However, as the U.S. and China do not have an extradition treaty, Liu remains in China, and it is very unlikely Liu will ever face trial. *Ph.D. Chemist Convicted Of Conspiracy To Commit Economic Espionage, Theft Of Trade Secrets, And Wire Fraud,* U.S. DEPT. OF JUST. (last visited Apr. 24, 2021) [hereinafter You Conviction], https://www.justice.gov/usao-edtn/pr/phd-chemist-convicted-conspiracy-commit-economic-espionage-theft-trade-secrets-and-wire.

i. Economic Espionage is (Not Only) a National Security Threat

Economic espionage is consistently framed as a threat to national security. And the premise underlying this thinking is simple–economic espionage threatens the economic well-being of the state which in turn threatens national security. This is how the United States has approached the issue since the mid-nineties,[32] and it is a decidedly post-Cold War way of thinking. The collapse of the Soviet Union reminded everyone that national power is not only determined by the strength of the nation's military but by the strength of the nation's economy as well.

Trade secrets are of particular importance to economies like that of the United States. As explained by the National Institute of Standards and Technology (NIST):

> In some ways, like companies, countries compete, economically, based on two primary methods: cost and differentiation. The U.S. tends to produce high-cost high-quality goods, making it more of a differentiator than a cost competitor. For differentiators, protection of intellectual property is critical; otherwise, competitors can simply commandeer those things that differentiate one competitor from another.[33]

The U.S. economy is dependent on the production of differentiated goods–on innovation and on technological advancement. That is why the value-added of IP-intensive industries accounts for so much of U.S. GDP. And producing high-cost, high-quality goods is expensive. When a foreign government steals U.S. trade secrets it enables its own companies to forgo the research and development costs paid by U.S. firms; it enables its companies to introduce market-competitive goods that may well be cheaper than the analogous U.S. goods because the foreign company did not ultimately have to

[32] *E.g.* ONCIX 1996 Report, *supra* note 18.
[33] DOUGLAS THOMAS, DEP'T OF COMM. NAT'L INST. OF STANDARDS AND TECH., MAN. SER. 100-32, CYBERCRIME LOSSES: AN EXAMINATION OF U.S. MANUFACTURING AND THE TOTAL ECONOMY (2020) [hereinafter NIST Report] https://nvlpubs.nist.gov/nistpubs/ams/NIST.AMS.100-32.pdf.

pay as much to produce the goods. This unfair competition will hurt revenue, jobs, and ultimately the U.S. economy. And that is why economic espionage poses a particularly acute threat to the United States and to other "differentiator" countries.

Depending on the nature of the trade secrets stolen, economic espionage can also result in traditional security consequences. In 2007, a hacking unit of China's People's Liberation Army (PLA) stole multiple terabytes of data about Lockheed Martin's F-35 Lightning II joint strike fighter jet.[34] The data was then passed to the Aviation Industry Corporation of China (AVIC), a state-owned aerospace company. From there, the data likely made its way to Chengdu and Shenyang subsidiaries of AVIC that went on to produce the J-20 and J-31 stealth fighters, respectively. Experts assert that both aircraft were built with the help of the stolen data about the F-35.[35]

The exfiltration of the F-35 data was part of a nearly decade-long series of operations by the PLA. The operations, dubbed, Byzantine Hades, successfully targeted both government and private sector systems to obtain information about sensitive defense technologies. In addition to the data relating to the F-35, China was also able to obtain data on the B-2 stealth bomber, the F-22 jet, space-based lasers, missile navigation and tracking systems, as well as nuclear submarine and anti-air missile designs.[36] The Byzantine Hades hacks are estimated to have done over $100 million in damage overall.[37]

---

[34] Franz-Stefan Gady, "New Snowden Documents Reveal Chinese Behind F-35 Hack," THE DIPLOMAT (Jan. 27, 2015), https://thediplomat.com/2015/01/new-snowden-documents-reveal-chinese-behind-f-35-hack/.
[35] *Id.*
[36] *Id.*
[37] *Id.*

The Byzantine Hades hacks are a great example of why economic espionage poses a threat to national security. But there is also a fundamental problem with framing economic espionage as a national security issue. The problem is that this threat cannot be effectively *addressed* by traditional national security actors alone. China stole the F-35 data from Lockheed Martin. The frontline defense against this act of economic espionage was a private company–a top U.S. defense contractor–but a private company, nonetheless. And while the Department of Defense does set some cybersecurity requirements for companies like Lockheed that make up the Defense Industrial Base (DIB),[38] Lockheed's network security is ultimately Lockheed's responsibility. And to be clear, the vast majority of U.S. businesses are not near as sophisticated as Lockheed Martin when it comes to cybersecurity. It is important to recognize the national security implications of economic espionage; but it is also important to recognize that the private sector will have to bear a great deal of the burden when it comes to defending against this threat.

ii. Economic Espionage is Not Traditional Espionage

When a state engages in economic espionage, is that activity really any different from the state's other espionage activities? According to U.S. law and policy, yes; economic espionage is distinct from traditional espionage. Espionage is a means of collecting intelligence; it is "one aspect of a nation's intelligence work, encompassing the government's efforts to acquire classified or otherwise protected information in order to deal with threats from actual or potential adversaries."[39] The U.S. view is that

[38] *See* 32 C.F.R. § 236 (containing the Department of Defense (DoD) DIB Cyber Security Activities including mandatory reporting requirements defense contractors in certain circumstances).
[39] Lotrionte, *supra* note 26, at 460.

economic espionage is not normal espionage. As explained by former National Security Advisor, Susan Rice:

> "[t]he issue is not about spying: frankly, we know (and they know) that we spy on each other as best we can through cyber and other means. In my business, espionage is fair game. What is utterly unacceptable to the U.S. is cyber theft of private company information for commercial gain."[40]

Rice's explanation suggests that the harm of economic espionage does not comes from the theft but rather the subsequent use of private sector data. States spy on each other; states steal secrets. Virtually every nation has some kind of intelligence service–civilian, military, and often both.[41] But economic espionage is different.

While the United States engages in espionage, it does not engage in economic espionage. The U.S. intelligence community (IC) maintains its distance from the U.S. private sector. So, while the IC collects economic intelligence about foreign nations and companies, it does not disseminate that intelligence to U.S. businesses.[42] And not all states recognize this distinction; every nation practices intelligence in ways that are specific–if not unique–to that nation.[43] Intelligence services are shaped by a nation's history, needs, preferences, and governmental structures.[44] A cynical explanation might suggest that the U.S. only chooses to draw a line between these activities because it feels it has more to lose than to gain when it comes to economic espionage. With more

---

[40] SUSAN RICE, TOUGH LOVE: MY STORY OF THE THINGS WORTH FIGHTING FOR 437 (Simon & Schuster, 2019).
[41] MARK M. LOWENTHAL, INTELLIGENCE: FROM SECRETS TO POLICY 489 (7th ed. 2017).
[42] In the 1980s there was some support for closer IC-private sector ties, but even proponents of that position were unable to answer questions about how such a relationship would work. If the IC were to share intelligence with businesses, how would businesses safeguard the sources and methods used in obtaining the information? Which U.S. companies would receive information? Which industries? Which entities even count as U.S. companies in our era of multinational corporations? Lowenthal quotes Gen. Gates as having responded to the idea by saying no U.S. intelligence officer was "willing to die for General Motors." *Id.* at 419-20.
[43] LOWENTHAL, *supra* note 41, at 13.
[44] Lotrionte, *supra* note 26, at 489.

than 38% of GDP coming from IP-intensive industries, the U.S. is certainly a target-rich environment. However, there are three important differences between economic espionage and traditional espionage that support distinguishing the two.

First, economic espionage serves a different purpose. The fundamental purpose of economic espionage is to garner a competitive advantage; it is for commercial gain. By contrast, the fundamental purpose of traditional espionage is to garner intelligence that will provide support to policymakers as they make decisions relating to national security. Intelligence is collected and analyzed largely for four major reasons: (1) to avoid strategic surprise; (2) to provide long-term expertise; (3) to support the policy process; and (4) to maintain the secrecy of information, needs, and methods.[45] Notably absent on that list is any reason resembling financial gain.

Second, economic espionage has a different impact on states and on relations between states. Economic espionage is a zero-sum game: "one foreign nation is deprived of its trade secrets while another benefits from its neighbor's sweat equity."[46] This has a destabilizing effect on relations between states. Traditional espionage is not necessarily a zero-sum game: in fact, "traditional espionage can serve to increase the security of states, helping to decrease the chances of surprise attacks and minimizing conflict, thereby preserving global security."[47] States can use the intelligence they gather to better understand the thinking of adversaries; to reduce tensions; to support cooperation; and to stabilize relations between states.[48]

[45] *Id.* at 2.
[46] Reid, *supra* note 22, at 761.
[47] Lotrionte, *supra* note 26, at 487.
[48] *Id. at 445.*

Third, economic espionage is different as a matter of law. Both economic espionage and traditional espionage are criminalized in domestic and foreign law. But traditional espionage is also *affirmatively* authorized and regulated in those same bodies of law. States openly acknowledge that they engage in traditional espionage. By contrast, as pointed out by Dr. Catherine Lotrionte, states that utilize economic espionage "have never openly acknowledged or enacted domestic laws authorizing government agencies to steal trade secrets from another state's corporations in order to directly benefit [their domestic businesses]."[49] States are far less candid about engaging in economic espionage.

It may seem somewhat hypocritical that states both reserve the right to engage in traditional espionage and the right to prosecute foreign spies. But it is a reflection of how traditional espionage is handled in customary international law. No body of international law makes a determination one way or another as to the legality of traditional espionage.[50] But espionage is useful; espionage can be mutually beneficial. The behavior of states seems to both recognize that and suggest that espionage is permissible within some normative limits. When a spy is captured, the nations involved will barter and make agreements for the spy to be returned home; they might exchange captured spies; they might expel foreign government officials outed for engaging in espionage as *personas non grata*.[51] But, most of the time, states will cooperate to avoid

[49] *Id.* at 488.
[50] This is true of peacetime intelligence; the permissibility of wartime intelligence is discussed in relation to the law of armed conflict. *Id.* at 473.
[51] *Id.* at 477-8.

public prosecutions.[52] They cooperate in order to preserve the mutual security benefits provided by traditional espionage and to create a custom of reciprocity.

But that is not the case with economic espionage. States simply do not have the same interest in cooperation in this context because there is no mutual benefit, and there is no common need for reciprocity. This is evident in the way states have responded to the problem so far. The United States very publicly indicts and (when it can) prosecutes individuals suspected to have stolen trade secrets for foreign governments. The U.S. response indicates that economic espionage lies outside the normative bounds of what states consider permissible when it comes to traditional espionage.

iii. How Cyber Capabilities Impact the Threat

The way states are stealing information has changed. Today, rather than being carried out by the co-opted factory worker with a pinhole camera, economic espionage is very often carried out through cyber operations.[53] How, if at all, do cyber capabilities change the economic espionage threat?

Cyber capabilities have certainly changed the lingo associated with economic espionage, but cyber capabilities have not changed the underlying nature of the threat. Nor have they necessarily changed the way states should address the threat at law.[54] The purpose of economic espionage is the same in cyberspace as in the physical

[52] Lotrionte, *supra* note 26, at 460.
[53] Though cyber is far from being the only means by which states conduct economic espionage. "Sophisticaed threat actors, such as adversarial nation-states, combine cyber exploitation with supply-chain operations, human recruitment, and the acquisition of knowledge by foreign students in U.S. universities, as part of a strategic technology acquisition program." NSCS Report 2018, *supra* note 25, at 4.
[54] Though it should be noted that when economic espionage *is* cyber-enabled, then, in addition to violating laws specific to the theft of trade secrets, the activity may also violate cyber-specific criminal laws such as the Computer Fraud and Abuse Act (CFAA).

world– economic espionage is still about commercial gain. And the way the U.S. and other states have criminalized economic espionage is–and should be–technology neutral. *Cyber* economic espionage is simply the latest evolution of an existing threat. And, as the threat continues to change with the times and technology, statutes criminalizing the theft of trade secrets should be capacious enough to account for those changes.

Cyber capabilities make stealing information easier, but cyber capabilities do not make stealing information any more effective. There is an assumption that moving economic espionage into cyberspace has necessarily advantaged the thief on both fronts, but that simply is not the case. The attack surface has increased exponentially alongside digitization. Between 1997 and 2017 the U.S. digital economy grew at a compound annual rate of 9.9% compared to a total growth rate of only 2.3% annually.[55] There is a growing abundance of data to steal. Cyber tools are also relatively low cost and low risk for the wielder; it is both less costly and less risky to send a phishing email than to employ a human source. So, in our "age of malware, botnets, rootkits, zero-day, honeypots, cybercriminal threats, advanced persistent threats (APTs)[,] and computer network exploitation," it is *easier* for adversaries to exfiltrate data.[56]

But, as posited by Thomas Rid, cyber capabilities do not necessarily make attempts at economic espionage more *effective*:

> "[R]emotely stealing *and then taking advantage of* trade secrets by clandestinely breaching a competitor's computer networks is more complicated than meets the eye."[57] Whether the exfiltrated data will actually strip a target of their competitive advantage largely depends on the *nature* of the data exfiltrated: "process-related

[55] NIST Report, *supra* note 33 at 4.
[56] Reid, *supra* note 22, at 763-4.
[57] THOMAS RID, CYBER WAR WILL NOT TAKE PLACE 82 (Oxford University Press, 2013).

> knowledge (think: bread making) may reside more in routines and practices, not in reports on hard-drives, and therefore seems to be more difficult to steal and to replicate remotely–whereas confidential data about acquisitions and business-to-business negotiations may be pilfered from top executives and exploited more easily."[58]

Targets can make economic espionage less effective by identifying and protecting the data that has the most competitive value. In order to do that, companies have to understand the value of what is at stake; they have to develop priorities when it comes to organizing information; and they have to take advantage of new technologies. The goal should be to make offensive cyber operations both more costly and more time consuming for would-be attackers. [59] Cyber capabilities do not have to be an offensive advantage. That being said, better cyber defense comes at a substantial (and growing) cost to businesses. The U.S. government, for its part, should do what it can both to incentivize better defense and make better defense more accessible.

iv. How Different States Approach Economic Espionage

Given the United States' dependence on IP-intensive industries, it is particularly vulnerable to economic espionage, but it is far from being the only country to struggle with the threat. Nearly all countries–developed and developing–have been victims of economic espionage.[60] However, while the U.S. and others have vehemently denounced the use of economic espionage, "differences in national pride, cultural, historical and nationalistic backgrounds, and economic and political governance allow

[58] *Id.* at 85.
[59] RICHARD A. CLARKE & ROBERT K. KNAKE, THE FIFTH DOMAIN: DEFENDING OUR COUNTRY, OUR COMPANIES, AND OURSELVES IN THE AGE OF CYBER THREATS 9 (Penguin Press, 2019).
[60] Reid, *supra* note 22, at 772.,

some countries to be unapologetic supporters of state-sponsored economic espionage."[61]

Many foreign countries have criminalized this kind of behavior in some form.[62] However, only Canada and New Zealand have specifically criminalized the misuse of trade secrets as the U.S. has in the EEA.[63] Other countries–including Argentina, Brazil, China, France, Germany, Italy, Japan, South Korea, Russia, Switzerland, Taiwan–apply other, existing criminal laws–such as for offenses relating to unfair practices–to prosecute the theft.[64] But, like the U.S., foreign countries have not had much success prosecuting individuals for state-sponsored acts of trade secret theft.[65]

Notably, some of the same countries on the list above are also prevalent users of economic espionage. The intelligence services of Russia, China, France–and additionally India and Israel–regularly provide foreign proprietary information to their domestic companies.[66] The relationships between intelligence agencies and businesses in these countries are somewhat of a natural byproduct of the state's proximity to industry. They likely see this as a normal function of intelligence because of the way the government is set up in relation to domestic business.

For many of these countries, economic espionage is seen as an effective way to speed up economic development. A number of international actors have justified this reasoning by drawing historical comparisons between modern economic espionage and

---

[61] *Id.* at 765.
[62] *Id.* at 773-76.
[63] *Id.* at 772.
[64] Noticeably absent from this list are the U.K. and Australia–despite being Five Eyes countries, have the UK or Australia has criminalized economic espionage. Both rely on civil proceedings and remedies for enforcement. *Id.* at 773-80.
[65] *Id.* at 772.
[66]Reid, *supra* note 22, at 784-802.

American corporate espionage in the industrial revolution.[67] The most oft-cited example is that of Francis Cabot Lowell in the early 1800s; Lowell, a merchant from Massachusetts, traveled to the U.K., memorized as much as he could about power looms, came back to the U.S., hired a master mechanic, and ultimately was instrumental in bringing the industrial revolution to the United States.[68] There is something to be said for the fact that Lowell's actions do not represent an act of *economic espionage*; they represent an act of industrial espionage–theft by a private competitor, not formally affiliated with a foreign government–for which he should have (and almost was) prosecuted.[69] But regardless, many state sponsors of economic espionage do not consider their conduct today to be any morally or substantively worse than Lowell's.

B. QUANTIFYING ECONOMIC ESPIONAGE

Quantifying the impact of economic espionage is a tremendously difficult task. The 2017 Update to the IP Commission Report estimated the cost of trade secret theft to the U.S. economy to be between $180 billion and $540 billion.[70] But loss estimates vary, and too often, an estimate will be adopted without much acknowledgement of the data problems that plague economic espionage and cybercrime,[71] more generally.

---

[67] Brenner, *supra* note 16, at 395.
[68] *Id.*
[69] On the way back from England Lowell and his family were detained and searched on suspicion of stealing secrets; luckily for Lowell, he had memorized rather than copied the information. Charles R. Morris, *We Were Pirates, Too*, FOREIGN POL'Y (Dec. 6, 2012), https://foreignpolicy.com/2012/12/06/we-were-pirates-too/.
[70] CTR. FOR STRATEGIC INT'L STUD., THE ECONOMIC IMPACT OF CYBERCRIME–NO SLOWING DOWN 8 (2018) [hereinafter CSIS 2018] https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf.
[71]Loss estimates relating to cybercrime will be both over and underinclusive when it comes to economic espionage. Cybercrime estimates will account for a host of different cyber problems–not just IP and trade secret theft. At the same time, cybercrime estimates will not account for those instances of theft that are not cyber enabled.

A 2020 report by NIST economist Douglas Thomas–entitled Cybercrime Losses: An Examination of U.S. Manufacturing and the Total Economy–provides a thorough discussion of loss estimate variation in some of the most prominent studies of cybercrime data.[72] The studies evaluated include a 2008 study by the Bureau of Justice Statistics; a 2014 study by PricewaterhouseCoopers, a 2018 study by the Council of Economic Advisers; a 2018 study by the Center for Strategic International Studies (CSIS) in conjunction with McAfee; and a 2019 study by Accenture Security and the Ponenmon Institute.[73] Of these studies, the most statistically reliable was determined to be the Bureau of Justice Statistics study, which surveyed 36,000 businesses in 2005 with 8,079 responses. When approximated to account for uncertainty, the results of that study suggested that losses from cybercrime in 2016 were between $167.9 billion and $770 billion. This finding was consistent with the hypothesis that widely cited estimates are actually *underestimating* losses from cybercrime.[74]

But some scholars suggest that estimates of cybercrime losses "are so compromised and biased that no faith whatever can be placed in their findings."[75] While that position is bleak and somewhat extreme, it is not without merit. One problem with estimates is that they usually do not provide much in the way of methodology, and they are often intentionally vague about what they measure and who they have surveyed.[76] But the bigger problem–the reason studies are vague and lack transparency as to methods–is that estimates face severe data limitations.

---

[72] NIST Report, *supra* note 33 at i.
[73] *Id.* at 8.
[74] *Id.* at i.
[75] DIEI FLORENCIO & CORMAC HERLEY, SEX LIES AND CYBER-CRIME SURVEYS 8 (Microsoft Research, 2011).
[76] *Id.*; NIST Report, *supra* note 33 at i.

The most significant limitation is underreporting.[77] Trade secret theft and other cybercrimes are critically underreported in the U.S. and globally.[78] In some cases, companies do not report because they do not realize they have anything to report. Companies may not realize that their data has been stolen; they may not even know they have been hacked.[79] But in many cases, companies do not report because they do not have to, and they do not want to. With very few exceptions,[80] U.S. companies are not required to report incidents of trade secret theft. The U.S. government also does not engage in any kind of systematic collection of public data on cybercrime.[81] Nor do companies have any real incentive to report trade secret losses.[82] In many instances, the private interests of the company will weigh against reporting the loss. Being hacked is already bad for business, but companies also do not want to risk any further public disclosure of their trade secrets.

The second limitation has to do with valuation. Assessing the value of intellectual property is a difficult task; but assessing the true cost of losses is impossible. As explained in 2018 CSIS report on the economic impact of cybercrime–

> Putting a value on IP is an art. How much is spent on research and development does not determine the value of IP. Companies can estimate what the IP would fetch on the market if offered for sale or licensing. Companies can estimate the future revenue stream their IP will produce. Extracting information from a computer network does not always mean there is immediate benefit to those who acquire the IP. Many high-tech products require significant "know-how" and experience to

[77] CSIS 2018, *supra* note 59, at 8.
[78] *Id.*
[79] DENNIS C. BLAIR & JON M. HUNTSMAN, JR., UPDATE TO THE IP COMMISSION REPORT: THE THEFT OF AMERICAN INTELLECTUAL PROPERTY REASSESSMENTS OF THE CHALLENGE AND UNITED STATES POLICY 2 (2017) [hereinafter UIPCR 2017].
[80] Such as the DIB requirements noted earlier. For example, DoD contractors are required to report incidents that affect covered information systems, covered defense information, or their ability to provide operationally critical support. *See* 32 C.F.R. § 236.
[81] NIST Report, *supra* note 33 at 8.
[82] UIPCR 2017, *supra* note 68 at 2.

> produce, and stolen IP alone does not provide that. A thief may not be able to make commercial use of the IP, and there may be a long lag between theft and the introduction of a competing product.[83]

It is not possible to predict whether and to what extent an adversary will be able to monetize stolen trade secrets. But in the meantime, the company will pay the "second-order"[84] or "hidden"[85] costs associated with economic espionage. These are the costs that estimates simply cannot account for. The company may have to pay recovery costs to clean up after the crime; the company may–hopefully–spend more than it otherwise would on cybersecurity and other forms of trade secret protection; the company may forgo opportunities that it otherwise would have pursued.[86] Perhaps the worst consequence is that the theft of trade secrets may result in chilling innovation.

These data limitations explain the variation in loss estimates. And while valuation will always be a problem, increasing reporting could do a great deal to help better illustrate the scale and scope of the problem. But as explained by the IP Commission report in 2013, "[w]hat is indisputable is that the scale and scope of the loss is enormous . . . . Even more important than the scale and scope of the loss is an overwhelming assessment by experts that current legal and regulatory approaches to mitigating the loss are staggeringly ineffective."[87]

IV. ASSESSING THE U.S. RESPONSE

The United States uses a mix of legal and policy tools to address the threat of economic espionage. The most prominent of those tools has long been the Economic

[83] CSIS 2018, *supra* note 59, at 17.
[84] UIPCR 2017, *supra* note 68, at 2.
[85] CSIS 2018, *supra* note 59, at 19.
[86] *Id.*; UIPCR 2017, *supra* note 68, at 2.
[87] IPCR 2013, *supra* note 8, at 22-3.

Espionage Act, which criminalizes state-sponsored trade secret theft.[88] However, the EEA is notoriously hard to enforce.[89] Since its passage in 1996, very few people have been prosecuted and even fewer have been convicted under the statute.[90] So the EEA's lasting relevance doesn't come from prosecutions or convictions; its lasting relevance comes from the Justice Department's use of indictments under the EEA and other related charges to name-and-shame foreign hackers. But this strategy, and the criminalization approach more generally, have been widely criticized,[91] and for good reason. Economic espionage certainly poses a bigger threat today than it did at the time of the EEA's enactment.

However, the U.S. does not rely on the EEA alone in its response to economic espionage. In recent years, the U.S. has employed a number of additional tools in civil law, diplomacy, and trade policy to react to economic espionage. But ultimately, the problem persists. The new federal private right of action faces 'reach' issues similar to those of the EEA; diplomatic agreements thus far between the U.S. and China have failed to lastingly curb IP theft; nor have trade tariffs stemmed China's behavior.

The U.S. government also engages in a number of activities designed to *prevent* economic espionage. The U.S. government is responsible for protecting its own networks. Additionally, the U.S. government offers opportunities for public/private partnership and information sharing about threats, vulnerabilities and other risks; it provides training and education programs on cybersecurity and information security to

[88] 18 U.S.C. 1831(a) (2012).
[89] IPCR 2013, *supra* note 8, at 41.
[90] Reid, *supra* note 22, at 771.
[91] *See* Robin L. Kuntz, *How Not to Catch a Thief: Why the Economic Espionage Act Fails to Protect American Trade Secrets*, 28 BERKELEY TECH. L.J. 901, 902 (2013); Hinck, *supra* note 23.

private industry; it provides guidance on current best-practices. But the value of these efforts is dependent on voluntary engagement by businesses. The U.S. government cannot protect private sector networks; it lacks both the resources and the authority. There is no statutory or regulatory mandate to meet certain security standards. Preventing economic espionage therefore is a responsibility largely left to U.S. businesses.

A. THE ECONOMIC ESPIONAGE ACT

The EEA was passed with near unanimous support and a considerable amount of fanfare in October 1996.[92] The digital economy was growing; technology was changing; and Congress was worried about IP and trade secret theft. In the years leading up to the EEA's enactment, the U.S. IC provided a number of reports suggesting that more than a dozen countries were actively targeting U.S. proprietary information and critical technologies.[93] The EEA's legislative history indicates that Congress was particularly concerned with this state-sponsored threat.[94] The EEA was intended to address the problem and to fill the otherwise existing gap in federal criminal law when it came to protecting proprietary information.[95]

---

[92] The EEA originated in the house and initially passed 399-3 (31 not voting). The bill was then passed by unanimous consent with changes in the Senate; passed without objection with changes in the House; and then finally passed by unanimous consent in the Senate and sent to the President. H.R. 3723 (104TH): ECONOMIC ESPIONAGE ACT OF 1996, https://www.govtrack.us/congress/bills/104/hr3723; President Clinton signed the bill into law and issued a statement asserting–"[t]oday I have signed into law H.R. 3723, the ''Economic Espionage Act of 1996.'' It strengthens our protections against the theft or misuse of proprietary business information. It will help U.S. crack down on acts like software piracy and copyright infringement that cost American businesses billions of dollars in lost revenues. And it will advance our national security." President William Clinton, Statement on Signing the Economic Espionage Act of 1996 (Oct. 11, 1996), https://www.govinfo.gov/content/pkg/WCPD-1996-10-14/pdf/WCPD-1996-10-14-Pg2040-2.pdf.

[93] ONCIX 1996, *supra* note 18, at 1.

[94] *See* Kuntz, *supra* note 80, at 902 (citing 142 Cong. Rec. H10,461 (daily ed. Sep. 17, 1996)).

[95] The earliest federal protections for U.S. IP can be found in Art. I, Sect. 8, Cl. 8 of the Constitution and the Patent Act of 1790. And even prior to the EEA, most states had adopted some form of the Uniform Trade Secrets Act which provided a private right of action in tort for the improper misappropriation of a

The EEA establishes two prosecutable offenses. Section 1831 criminalizes "Economic Espionage"–the act of intentionally or knowingly stealing or receiving a trade secret for the benefit of a foreign government, foreign instrumentality, or foreign agent.[96] Section 1832 criminalizes "Theft of Trade Secrets"–the act of stealing or receiving a trade secret with the intent to benefit anyone who is not otherwise authorized to use the trade secret.[97] For purposes of both 1831 and 1832, "trade secret" is defined broadly to include–

---

trade secret. However, before the EEA there was no federal legislation that specifically addressed the threat of trade secret theft. Other criminal statutes–such as the Interstate Transportation of Stolen Property Act (ITSPA)–were sometimes used to prosecute trade secret theft, but by the 1990s many of these statutes proved too outdated to be of much use. For example, ITSPA criminalizes the use of an automobile to transport goods, wares, or merchandise over state lines. James M. Fischer, *Note: An Analysis of Economic Espionage Act of 1996*, 25 SETON HALL LEGIS. J. 239, 248-256 (2001).

[96] 18 U.S.C. 1831(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. 18 U.S.C. § 1831 (2012).

[97] 18 U.S.C. 1832 (a)Whoever, with intent to convert a trade secret, that is related to a product or service used in or intended for use in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly—

> (1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information;

> 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 [so long] the owner thereof has taken reasonable measures to keep such information secret [and] the information [has independent economic value[98] because it is secret].[99]

Importantly, neither 1831 nor 1832 protects against negligent or reckless transfer of trade secrets. 1831 requires the violator to act with intent or knowledge; and 1832 requires intent. Potential penalties under the EEA include imprisonment, fines, criminal forfeiture, and injunctive relief. Economic espionage carries a maximum sentence of fifteen years imprisonment; trade secret theft carries a maximum sentence of ten years.[100]

> (2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information;
>
> (3) receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;
>
> (4) attempts to commit any offense described in paragraphs (1) through (3); or
>
> (5) conspires with one or more other persons to commit any offense described in paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy, shall, except as provided in subsection (b), be fined under this title or imprisoned not more than 10 years, or both.

(b)Any organization that commits any offense described in subsection (a) shall be fined not more than the greater of $5,000,000 or 3 times the value of the stolen trade secret to the organization, including expenses for research and design and other costs of reproducing the trade secret that the organization has thereby avoided. 18 U.S.C. § 1832 (2016).

[98] The company need not have actually suffered loss; it is enough that the independent economic value be "potential" rather than actual. United States v. Hanjuan Jin, 773 F.3d 718, 720 (7 Cir. 2013).

[99] 18 U.S.C. § 1839(3) (2016).

[100] The EEA was amended in 2013 to increase the monetary fines available under the statute.[100] Under 1831, for individual defendants, the penalty was raised from $500,000 to $5 million, and for organizations, the penalty was raised from $10 million to the greater of $10 million or three times the value of the stolen trade secrets. These changes reflect recognition on the part of the U.S. government of the growing scope and scale of the threat. Foreign and Economic Espionage Penalty Enhancement Act of 2012, Pub. L. No. 112-269, 126 Stat. 2442. (2013); Reid, *supra* note 22 at 768.

But what really distinguishes 1831 from 1832 is *who must benefit* from the theft. Under 1831, the theft must be for the benefit of a foreign government, instrumentality, or agent.[101] Under 1832, the theft only need be for the benefit of someone without authorization to use the trade secret. So, while 1832 applies to protect businesses and government entities from corporate espionage and private competitors, 1831 applies only when the thief intended for or knew that a foreign power would ultimately benefit.

Now having established the law, it is time to explain why it has been ineffective. The EEA has not curbed the economic espionage problem. As established, economic espionage is a bigger problem today than it was in 1996. But more specifically, the EEA, and in particular section 1831, is not an effective tool to provide criminal punishment or criminal deterrence for state-sponsored acts of trade theft. Section 1831 is tremendously difficult to enforce. In the twenty-five years since the EEA was enacted, there have only been nine convictions under section 1831 for which information is publicly available.

The following table lists the details of known economic espionage convictions. This table is based on publicly available data[102] provided on the "Federal Cases" database compiled by Dr. Jeremy Wu,[103] and it is supplemented by Melanie Reid's

[101] A "foreign instrumentality" is any agency, bureau, ministry, component, institution, 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; a "foreign agent" is any officer, employee, proxy, servant, delegate, or representative of a foreign government. 18 U.S.C. 1939(1-2) (2016).

[102] Data on economic espionage convictions is hard to find; databases and reports like those cited below are wonderful resources, but they are not official sources. Information about convictions comes from DOJ's selective public reporting and the news. This data gap is ripe for research. Data-driven research about enforcement efforts and prosecutions could be very helpful in evaluating the efficacy of criminal indictments and prosecutions.

[103] The "Federal Cases" database was created by Dr. Jeremy Wu, a retired senior advisor at the U.S. Census Bureau. The database compiles shared, publicly available information about economic espionage prosecutions and is part of Wu's broader Asian-American advocacy efforts. Jeremy S. Wu, "Federal

2016 article, “A Comparative Approach to Economic Espionage: Is Any Nation Effectively Dealing With This Global Threat.”[104]

Table 1: 18 U.S.C. § 1831 Convictions, 1996-2021

YEAR	CASE	COURT	COMPANY	COUNTRY	SENTENCE
2002; 2006	United States v. Fei Ye; Ming Zhong	N.D. CA; 9 Cir. COA	NEC Electronics; Sun Microsystems Inc.	China	1 Yr. Prison
2006	United States v. Xiaodong Meng	N.D. CA	Transmeta Corporation Quantum 3D, Inc.	China; Thailand; Malaysia	2 Yr. Prison
2008; 2011	United States v. Dongfan “Greg” Chung	C.D. CA; 9 Cir. COA	The Boeing Company	China	188 Mo. Prison; 3 Yr. Supervised Release
2011	United States v. Kexue Huang	S.D. IN	Dow AgroSciences; Cargil, Inc.	China; Japan	87 Mo. Prison, 3 Yr. Supervised Release
2011	United States v. Elliot Doxer	D. MA	Akami Technologies, Inc.	Israel	6 Mo. Prison; 2 Yr. Supervised Release; $25,000 Fine
2014	United States v. Walter Liew, & USA Performance Technology, Inc.	N.D. CA	E.I. du Pont de Nemours & Company [DuPont]	China	15 Yr. Prison; $511,667.82 Fine
2016	United States v. Jiaqiang Xu	S.D. NY	International Business Machines Corp. [IBM]	China	5 Yr. Prison
2018	United States v. Hao Zhang	N.D. CA	Avago Technologies; Skyworks Solutions, Inc.	China	18 Mo. Prison; $476,835 Fine
2021	United States v.	E.D. TN	Coca-Cola	China	Pending

Cases,” JEREMY S. WU, PHD (Last visited Apr. 23, 2021) https://jeremy-wu.info/fed-cases/ [hereinafter Federal Cases].

[104] Reid, *supra* note 22, at 771-2.

	Xiaorong "Shannon" You[105]				

These are the only cases that resulted in convictions for economic espionage. But they are far from being the only cases in which economic espionage was charged. In many cases, economic espionage will be one of many charges, and defendants will end up pleading to a less serious offense.[106] Other criminal statutes that are commonly found alongside economic espionage in an indictment include theft of trade secrets; mail or wire fraud;[107] foreign or interstate transportation of stolen property;[108] the Export Control Act[109] and the International Traffic in Arms Regulations (ITAR);[110] money laundering;[111] and the Computer Fraud and Abuse Act's Fraud Scheme.[112]

But again, if Congress's purpose in enacting the EEA–and specifically in creating the economic espionage offense–was to provide criminal punishment and criminal deterrence for state-sponsored acts of trade theft, then it has failed. There are two reasons why it is so difficult to enforce the EEA.

First, economic espionage is hard to prove at trial. There are only a few decisions that provide guidance on what section 1831 requires; but helpful discussions can be found in the Northern District of Illinois' trial decision in United States v. Hanjuan Jin[113]

---

[105] You Conviction, *supra* note 31.
[106] *E.g. Taiwan Company Pleads Guilty to Trade Secret Theft in Criminal Case Involving PRC State-Owned Company*, U.S. DEPT. OF JUST. (last visited Apr. 24, 2021) (discussing how United Microelectronics Corporation, Inc.–a Taiwan semiconductor foundry–plead guilty to theft of trade secrets and was sentenced to pay a $60 million fine) https://www.justice.gov/usao-ndca/pr/taiwan-company-pleads-guilty-trade-secret-theft-criminal-case-involving-prc-state-owned.
[107] 18 U.S.C. § 1341 (2008); 18 U.S.C. § 1343 (2008); 18 U.S.C. § 1346 (1988).
[108] 18 U.S.C. § 2314 (2013).
[109] 22 U.S.C. § 2778 (2014).
[110] 22 C.F.R. § 120 (2014).
[111] 18 U.S.C. § 1956 (2016); 18 U.S.C. § 1957 (2012).
[112] 18 U.S.C. § 1030 (2020); Reid, *supra* note 22, at 771-2.
[113] Wherein the defendant was found guilty of 1832 trade secret theft but was ultimately acquitted on the 1831 charge because the government did not establish benefit to a foreign government, instrumentality,

and the Northern District of California, San Jose Division's order in U.S. v. Lan Lee.[114] Many of the elements of economic espionage overlap with elements of trade secret theft.[115] However, economic espionage has an additional element–the defendant must have intended or known that her conduct would benefit a foreign government, instrumentality, or agent.[116] The element has been broken down into two inquiries.[117] The government first must prove that the intended beneficiary was in fact a foreign government, instrumentality or agent.[118] The term "foreign government" has been interpreted to mean "the entity that constitutes the governing body of a foreign country"; the term is not synonymous with broader terms like "foreign country" or "foreign company."[119] Then the government must prove that the defendant *intended* or *knew* her conduct would benefit such an entity. What constitutes a benefit is construed broadly. The government does not have to show that the victim suffered economic loss; the government only must show that the conduct would benefit the foreign government, instrumentality, or agent "'in any way.'"[120] But proving intent or knowledge beyond a reasonable doubt is a heavy burden.[121]

---

or agent. U.S. v. Hanjuan Jin, 833 F.Supp.2d 977, 1019-20 (N.D. Ill. 2012), *aff'd*, 733 F.3d 718 (7th Cir. 2013).

[114] Wherein the defendant was acquitted on counts relating to conspiracy to commit economic espionage because the government did not establish benefit to any foreign government. U.S. v. Lan Lee, No. CR 06-0424 JW, 2010 WL 8696087 (N.D. Cal. 2010).

[115] Overlapping elements include (1) whether something constitutes a trade secret for the purposes of the act; (2) whether the trade secret is not known or readily ascertainable; (3) whether the owner employed reasonable measures to maintain secrecy; (4) whether the trade secret has independent economic value; (5) whether the defendant knew she had a trade secret; and (6) whether the trade secret was misappropriated. *Hanjuan Jin*, 833 F.Supp.2d at 1006-19.

[116] *Id*. at 1019.

[117] *Id.*

[118] *Id.*

[119] *Lan Lee,* No. CR 06-0424 JW, 2010 WL 8696087 at 6.

[120] *Hanjuan Jin*, 833 F.Supp.2d at 1019 (citing H.R.Rep., No. 104-788, at 11).

[121] In U.S. v. Hanjuan Jin, the court held that the government failed to prove that the defendant intended or knew her conduct would benefit the PRC in any way. The government argued that the defendant knew that the recipient company of the stolen trade secrets develops technology for the Chinese military. However, this argument was not considered sufficient to show the defendant's intent or knowledge. *Id.*

Second, the territorial reach of the EEA very often exceeds the territorial reach of U.S. prosecutors and law enforcement authorities.[122] This complicates enforcement of both 1831 and 1832. The territorial limits of the EEA are broad–the EEA protects against theft that occurs both inside or outside the US.[123] But once a violator is overseas, there is very little a prosecutor can do to bring her into a U.S. court room.[124] This is especially true when violators are based in or flee to top economic espionage sponsors such as Russia, China, and Iran–none of whom share an extradition treaty with the United States. And regardless of whether there is an extradition treaty, state-sponsors of economic espionage have an overwhelming economic and political disincentive to hand violators over to the United States for prosecution.

B. THE INDICTMENT STRATEGY

Because the law is so hard to enforce, many charges under the EEA never make it past the indictment stage. But, regardless of whether the EEA is an effective criminal enforcement mechanism, some experts argue that indictments, especially of known state actors, have independent value more as a policy tool.

Indictments can be used to name-and-shame perpetrators of economic espionage. Indictments attribute acts of economic espionage both to the individual actor and to the corresponding foreign government. These nation-state-oriented indictments serve as a "warning to would-be hackers that the [US] government can gather

[122] IPCR 2013, *supra* note 8, at 42.
[123] Where, if the threat occurred outside the US, (i) the offender is a natural person who is a citizen or permanent resident alien of the United States, or an organization organized under the laws of the United States or a State or political subdivision thereof; or (ii) an act in furtherance of the offense was committed in the United States. 18 U.S.C. 1837 (1996).
[124] IPCR 2013, *supra* note 8, at 42.

undeniable evidence proving the attack [and identifying] the perpetrators."[125] As explained by Assistant Attorney General for National Security, "'What the government is saying is not only, 'We think this is happening' or 'We assess with a high likelihood this is happening,' but it's saying 'I can get up in court and prove every element of what I've laid out in this indictment beyond a reasonable doubt.'"[126] But is naming-and-shaming effective? Arrests are rarely made in these cases. Without a credible threat of subsequent enforcement, what does attribution accomplish? [127]

Many experts assert that it does not accomplish much at all. As Jack Goldsmith and Robert Williams have argued in Lawfare, "the strategy of charging Chinese hackers for theft of U.S. trade secrets has failed to deter such activity." [128] In May of 2014, the Justice Department indicted five PLA hackers for computer hacking, economic espionage, and other offenses directed at companies in the U.S. nuclear power, metals and solar products industries.[129] That was the first time criminal charges had ever been filed against known state actors for engaging in such behavior. [130] John Carlin, the then-Assistant Attorney General for National Security said of the indictments– "[s]tate actors engaged in cyber espionage for economic advantage are not immune from the law just because they hack from under the shadow of their country's flag."[131]

---

[125] David Hechler, *What is the Point of These Nation-State Indictments?* LAWFARE (Feb. 8, 2021), https://www.lawfareblog.com/what-point-these-nation-state-indictments.
[126] Derek B. Johnson, *DOJ official says 'name and shame' is one piece of the puzzle*, FWC (Jan. 18, 2019) (quoting AAG John Demers), https://fcw.com/articles/2019/01/18/demers-doj-cyber-shame.aspx.
[127] Though it should be pointed out that once indicted, foreign hackers cannot easily travel abroad. This is not an empty consequence, though it is certainly not as consequential as arrest or prosecution. *Id.*
[128] Hinck, *supra* note 23 (citing Jack Goldsmith and Robert Williams).
[129] *U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage*, U.S. DEPT. OF JUST. (last visited Feb. 8, 2021) [hereinafter PLA Indictments 2014] https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.
[130] *Id.*
[131] DAVID E. SANGER, THE PERFECT WEAPON: WAR SABOTAGE, AND FEAR IN THE CYBER AGE 120 (Crown 2018).

Since then, there have been many similar nation-state indictments issued against Russian, Iranian, North Korean, and Chinese state actors for economic espionage or other cybercrimes.[132] In 2018, the Justice Department seemingly doubled down on this strategy with regard to China; DOJ's National Security Division (NSD) launched the "China Initiative" under which it has increased efforts to identify and prosecute those engaged in trade secret theft sponsored by the PRC.[133] But increased indictments have not deterred state-sponsored trade secret theft. As suggested by Goldsmith, "[t]he United States has for six years been playing up its extraordinary intelligence capacity to attribute malicious cyber operations. And for six years the attacks have grown worse."[134]

Others argue that attribution is valuable because it disrupts economic espionage and other cyber operations. Carlin has suggested–

> We believe the value of bringing criminal charges against foreign hackers is more complicated than the arguments about their deterrent value have so far suggested. In our view, these actions are not without impact. In some cases, charges have led to the arrest of those accused and may deter individual hackers from working with particular states. At the same time, because arrests have been the exception and the charging documents are primarily "speaking indictments" that communicate important details about hacking operations to the public, we conclude that charging foreign hackers, as well as online influence operators, serves purposes other than merely arresting specific individuals. We therefore distinguish between criminal charges as a tool for long-term deterrence versus as a tool for operational disruption.[135]

---

[132] Jack Goldsmith, *The Puzzle of the GRU Indictment*, LAWFARE (Oct. 21, 2020), https://www.lawfareblog.com/puzzle-gru-indictment.

[133] *Information About the Department Of Justice's China Initiative and A Compilation of China-Related Prosecutions Since 2018*, U.S. DEPT. OF JUST. (last visited Mar. 13, 2021) (explaining that "about 80 percent of all economic espionage prosecutions brought by the U.S. Department of Justice (DOJ) allege conduct that would benefit the Chinese state, and there is at least some nexus to China in around 60 percent of all trade secret theft cases.") [hereinafter China Initiative], https://www.justice.gov/nsd/information-about-department-justice-s-china-initiative-and-compilation-china-related.

[134] Hechler, *supra* note 114.

[135] Hinck, *supra* note 23.

Indictments might not deter future acts of economic espionage; but they can disrupt ongoing operations by the named actors. Indictments can bring public attention to hacking operations; depending on how detailed the indictment is, it may provide valuable information about the methods (and malware) being used to carry out the operation.

In sum, given that there is little potential for enforcement, indictments have little if any deterrent value. However, indictments are also not totally worthless. They can provide valuable, operational information about state actors and the methods those actors are using to steal American trade secrets. But much like broader criminalization efforts, indictments are insufficient on their own to meaningfully address the threat of economic espionage.

C. CIVIL ACTIONS AND THE DEFEND TRADE SECRETS ACT

Prior to 2016, another prevailing criticism of the EEA was that it did not provide a federal private right of action for victims of trade secret theft. There was no way, under federal law, for companies to sue in relation to the theft of their IP and other trade secrets.[136] Under the original language of the EEA, in section 1836, the attorney general could initiate civil proceedings seeking injunctive relief, but the EEA did not provide for any other form of civil action.[137] Enforcement was a choice left entirely up to prosecutors rather than victims. If the aggrieved trade secret holder wanted to sue, their only option was to bring a claim in state court. But–though most states have adopted some form of the Uniform Trade Secrets Act (UTSA)–trade secret law across states varies; and state

[136] IPCR 2013, *supra* note 8, at 5.
[137] *Id.*; Economic Espionage Act of 1996, Publ. L. 104-294, § 1836, 110 Stat. 3488, 3490 (1996).

courts came with their own complications "including limited access to evidence and difficulty enforcing judgments."[138]

In order to "replace [the] so-called 'patchwork of state trade secrets laws'" Congress enacted the Defend Trade Secrets Act (DTSA) in 2016.[139] The DTSA amended section 1836 to provide a federal private right of action for victims of trade secret theft.[140] Remedies available under the DTSA include: injunctive relief,

The DTSA was supposed to be a new way to encourage private industry to take action and a new way address trade secret theft at law. The law allows companies to make decisions about how and when to sue, and the hope is that (a) companies are able to recover and (b) that these civil suits will drive up the cost of trade secret theft for perpetrators. Importantly, the DTSA created protections for plaintiffs to conceal the nature of their trade secrets. As mentioned, one reason companies are reticent to report incidents of trade secret theft is because they want to avoid any further disclosure about their proprietary information. The inclusion of protective provisions in the DTSA was meant to ease these fears and encourage victims to pursue recourse in federal court.[141]

Courts have held that the DTSA can apply to extraterritorial defendants when an act in furtherance of the theft was committed in the United States.[142] Section 1837, which defines the territorial reach of the EEA, applies to the civil action in section 1836

---

[138] IPCR 2013, *supra* note 8, at 73.
[139] Danielle A. Duszczysyn & Daniel F. Roland, *Three Years Later: How the Defend Trade Secrets Act Complicated the Law Instead of Making it More Uniform* FINNEGAN (Jul. 2019), https://www.finnegan.com/en/insights/articles/three-years-later-how-the-defend-trade-secrets-act-complicated-the-law-instead-of-making-it-more-uniform.html.
[140] 18 U.S.C. § 1836(b)(1) An owner of a trade secret that is misappropriated may bring a civil action under this subsection if the trade secret is related to a product or service used in, or intended for use in, interstate or foreign commerce. 18 U.S.C. § 1836 (2016).
[141] UIPCR 2017, *supra* note 68, at 7.
[142] vPersonalize Inc. v. Magnetize Consultants Ltd., No. 2:18-CV-01836-BJR, 2020 WL 534505 (W.D. Wash. Feb. 3, 2020).

just as it applies to the criminal offenses in sections 1831 and 1832.[143] But the civil action suffers from the same enforcement problem as the criminal offenses. Just as it is hard to enforce criminal penalties, it will be hard to enforce civil judgements against perpetrators of cyber economic espionage. Therefore, while the DTSA may be a valuable tool for companies to recover in cases of corporate or industrial espionage;[144] the DTSA is unlikely to have much success as a tool to combat state-sponsored trade secret theft, especially as it may be carried out by state actors or officials.

D. BILATERAL AGREEMENTS AND TRADE MECHANISMS

In addition to the tools available at law, the U.S. government response includes a number of policy tools. Particularly, as China's use of economic espionage has garnered more attention and concern in the last decade, executive policies and actions have played a critical role in the U.S. government response. Diplomatic and economic efforts–including but certainly not limited to bilateral agreements and trade sanctions–played a big role in how the Obama and Trump administrations approached the problem. The Obama administration's approach to this threat can be characterized by its diplomatic efforts–executive policy under Obama is indicative of a more engagement-focused approach to the U.S.-China relationship, more broadly. By contrast, the Trump administration's approach can be characterized by its aggressive trade policy–this

[143] *Id.*

[144] There is some debate as to whether the addition of a federal right of action really added value to companies' attempts to recover after their trade secrets have been stolen. For example, as explained by Duszczysyn and Roland, DTSA claims are often brought alongside corresponding state claims. Whether for convenience, absence of contrary authority, or agreement of the parties to look to state law, courts often rely on the accompanying state law when analyzing DTSA claims. As a result, jurisdictions differ in their approaches to the DTSA. In sum, the DTSA did not accomplish much when it comes to uniformity. There is also reason to believe that the DTSA has increased costs for litigants–there is now more law to be familiar with; more procedural and substantive disputes to litigate; and more paperwork to be done. Duszczysyn, *supra* note 127.

policy is indicative of a more competition-focused approach Trump took both to the economic espionage threat and to the U.S.–China relationship. However, the executive policies of the last six years–including bilateral agreements and trade sanctions–have proven insufficient to provide a permanent solution to the threat of economic espionage.

In September of 2015–more than a year after the first set of PLA indictments was released[145]–President Obama entered into an agreement with President Xi that stated that neither the U.S. or the PRC would conduct or knowingly support cyber-enabled theft of intellectual property.[146] Though not legally-binding, the Agreement generated a lot of optimism about the future of norms creation in the cyber realm.[147] One month after the agreement, China entered into a similar agreement with the U.K., and two months after the Agreement, leaders at the G-20 conference endorsed similar language, committing to not conduct cyber-enabled economic espionage.[148]

The Agreement appeared to be successful in the short run; for about eighteen months, the volume of Chinese malicious cyber activities targeting the U.S. decreased.[149] The optimistic analysis of this trend is that the decrease was the direct result of the Agreement. However, many experts argue that might not have been the case. China's offensive operations did not stop; they just changed. As attested by the National Counterintelligence and Security Center in 2018, China's malicious cyber activity never totally stopped, and in particular, operations continued to target sensitive

[145] There is something to be said for indictments' capacity to signal the US's level of exasperation with an adversary's behavior. The 2014 indictments may have helped drive China to the negotiating table. But more commonly, the OPM hack–in which China obtained the security clearance files of 22 American officials, military personnel, contractors, and intelligence officers–is credited as being the impetus for the agreement. Sanger, *supra* note 11.
[146] Obama-Xi Agreement 2015, *supra* note 10.
[147] Joint Statement 2015, *supra* note 10.
[148] CSIS 2018, *supra* note 50, at 17.
[149] Sanger, *supra* note 11.

industry groups such as cleared defense contractors and IT and communications firms.[150] Chinese cyber operations were becoming more narrowly focused on critical technologies that could give the PRC both an economic and a military advantage.[151] The decrease in Chinese malicious cyber activity might not have been because of the new Agreement; it might have been because China had become a more sophisticated cyber actor. China no longer needed to hack *everything* when it could hack *anything*.[152]

Soon after President Trump took office, as tensions between the U.S. and China rose, Chinese hacking accelerated.[153] In August of 2017, growing concern over IP theft led the U.S. Trade Representative (USTR) to initiate an investigation[154] into "'whether acts, policies, and practices of the Government of China related to technology transfer, intellectual property, and innovation' were unreasonable or discriminatory, and burdened or restricted U.S. Commerce."[155] In March of 2018, the investigation concluded that a number of China's behaviors[156]–including unauthorized cyber

[150] NCSC 2018, *supra* note 25, at 7.
[151] Sanger, *supra* note 11.
[152] Adam Segal, *The U.S.-China Cyber Espionage Deal One Year Later*, COUNCIL ON FOREIGN REL. (Sep. 28, 2016) (quoting former NSA official, Dave Aitel), https://www.cfr.org/blog/us-china-cyber-espionage-deal-one-year-later.
[153] Sanger, supra note 11.
[154] This investigation was conducted pursuant to Section 301 of the Trade Act of 1974, which grants the USTR a number of authorities to investigate and enforce U.S. rights under trade agreements and in foreign trade practices. CONG. RES. SERV., INTELLECTUAL PROPERTY VIOLATIONS AND CHINA: LEGAL REMEDIES 1 (2020) [hereinafter CRS IP Violations Report].
[155] CONG. RES. SERV., SECT. 301 OF THE TRADE ACT OF 1974 1 (2021) [hereinafter CRS Trade Act Analysis].
[156] The USTR investigation concluded: "the (1) use of foreign ownership restrictions and administrative licensing requirements to pressure technology transfer from U.S. companies to Chinese entities; (2) IP licensing restrictions that discriminate against foreign entities; (3) systematic investment in or acquisition of U.S. companies to acquire targeted technologies; and (4) unauthorized cyber intrusions into U.S. networks to obtain IP and other confidential business information" constituted a violation of the Trade Act of 1974. OFF. OF THE U.S. TRADE REPRESENTATIVE, FINDINGS OF THE INVESTIGATION INTO CHINA'S ACTS, POLICIES, AND PRACTICE RELATED TO TECHNOLOGY TRANSFER, INTELLECTUAL PROPERTY, AND INNOVATION UNDER SECTION 301 OF THE TRADE ACT OF 1974 (2018), at 151–54, https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF; CRS IP Violations Report, *supra* note 144, at 2.

intrusions into U.S. networks to obtain IP and other confidential business information–constituted unfair practices in violation of the Trade Act of 1974.[157] And because China's actions violated the Trade Act of 1974, the Trump administration was empowered and entitled to respond.[158]

Beginning in early 2018, the U.S. imposed tariffs on a variety of Chinese exports; China responded in kind.[159] This trade war escalated for two years until the U.S. and China reached a new trade agreement–the Phase One Agreement–in February of 2020. Over the course of his presidency, Trump imposed hundreds of billions of dollars in tariffs on Chinese exports.[160] By the beginning of 2020, 66.4% of all Chinese exports were subject to U.S. tariffs.[161]

But tariffs have not proved effective in combatting cyber economic espionage. It is clear that the idea behind the strategy was that, by imposing tariffs on Chinese exports, the U.S. could shift the cost of China's unfair practices back onto China and

---

[157] *Id.* at 1-2.

[158] The Trump administration considered responses involving the WTO dispute resolution mechanism; trade tariffs; and executive actions relating for foreign investment. Specifically, in response to the USTR's conclusion about China's unfair licensing practices, the U.S. initiated a WTO dispute. Licensing practices and coercive technology transfer are outside the purview of this report, but the WTO dispute resolution mechanism has implications for economic espionage. The US alleged that the licensing practices violate China's WTO commitments and The Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) because the practices treat U.S. IP rights holders less favorably than Chinese IP rights holders. However, the dispute has been suspended (at the U.S.'s request) multiple times since initiated. *Id.* at 26. There are quite a few analyses that discuss using the WTO's dispute resolution mechanism to address economic espionage and trade secret theft. *E.g.* Lotrionte, *supra* note 26, at 524. However, as suggested by Lotrionte and the CRS Report on IP Violations, such efforts would most likely be ineffective to curtail economic espionage for three reasons (1) it is unclear whether economic espionage would be considered to violate TRIPS, and (2) even if it did, it would be very hard to prove, and (3) WTO members "retain some flexibility with regard to implementation and enforcement." CRS IP Violations Report, *supra* note 144, at 2.

[159] Chad P. Bown, *U.S. China Trade War Tariffs: An Up-to-Date Chart*, PETERSON INST. FOR INT'L ECON. (Mar. 16, 2021), https://www.piie.com/research/piie-charts/us-china-trade-war-tariffs-date-chart.

[160] *Id.*

[161] *Id.*

disincentivize further theft. But there are a few problems with taking a trade war-approach to economic espionage.

First, tariffs are often not an effective cost-shifting mechanism. U.S. tariffs are paid by U.S. importers. When importers have to pay more for foreign exports, they may choose to export from a different country–one that does not require the importer to pay such a high duty–but they may also just transfer the cost of the tariff onto the consumer through higher prices. Foreign companies may pay for the tariff indirectly either by losing business or by decreasing costs for US importers to make up for the higher duty; but the brunt of the cost is borne by US consumers.[162] The cost is even further removed when talking about the cost to the foreign government, itself.

Second, tariffs are an especially ineffective cost-shifting mechanism when it comes to cyber economic espionage. As explained earlier, cyber economic espionage is a very cost-effective activity for the state sponsor. It is low cost, low risk, and high reward. So long as (1) American consumers are paying for the brunt of tariffs, (2) the cost of offensive operations remains low, and (3) the pay-off from stealing trade secrets remains high, then tariffs cannot effectively disincentivize economic espionage.

Third, the trade-war approach to economic espionage fails to adequately distinguish the threat posed by economic espionage from concerns about private technology transfer. As explained by the New York Times' David Sanger and Steven Myers–

> Mr. Trump and administration officials often suggest that all technology-acquisition efforts by China amount to theft. In doing so, they are blurring the line between

[162] Rajesh Kumar Singh, *Explainer: Trump's China tariffs - Paid by U.S. importers, not by China*, REUTERS (Aug. 1, 2019), https://www.reuters.com/article/us-usa-trade-china-tariffs-explainer/explainer-trumps-china-tariffs-paid-by-u-s-importers-not-by-china-idUSKCN1UR5YZ.

> stealing technology and negotiated deals in which corporations agree to transfer technology to Chinese manufacturing or marketing partners in return for access to China's market — a practice American companies often view as a form of corporate blackmail but one distinct from outright theft.[163]

By conflating the two, the United States effectively undercuts the severity of the economic espionage threat. China's policies on data localization or foreign IP licensing may be undesirable; but companies are willingly agreeing to those policies as the cost of doing business in China. Companies are consciously making the choice to subject themselves to regulation by entering the Chinese market. The same cannot be said for economic espionage practices. In his recent book, *Chaos Under Heaven: Trump, Xi, and the Battle for the 21st Century,* Josh Rogin quips that "Trump, for his part, conflated the two[ ]all the time, mixing national security considerations and economic concessions and regular old favor trading in a way that made his officials crazy but made Xi Jinping very happy."[164] If the United States wants the international community to take this threat seriously, then the United States must take care to explain why state sponsored theft of proprietary information is particularly reprehensible.

Bilateral agreements are also unlikely to permanently solve the cyber economic espionage problem. As noted, in January of 2020, the US and China entered into a new bilateral agreement–the "Phase One Agreement," which provides that the U.S. and China must "ensure effective protection for trade secrets and confidential business information and effective enforcement against the misappropriation of such

[163] Sanger, *supra* note 11.
[164] JOSH ROGIN, CHAOS UNDER HEAVEN: TRUMP, XI, AND THE BATTLE FOR THE 21ST CENTURY 146 (Houghton Mifflin Harcourt, 2021) (referring to what he calls the "two wars," or the "trade war" and the "data war").

information."[165] But the future of the Phase One Agreement is entirely unclear right now. Due to the onset of COVID-19, the Phase One Agreement was not implemented on schedule, nor was a 'Phase Two' ever negotiated. In his first hundred days in office, President Biden has not publicly addressed the deal; and at present, there are not any talks currently scheduled between U.S. Trade Representative Katherine Tai and Chinese Vice-Premier Liu He despite the Agreement's stipulation for talks to occur every six months.[166]

What is clear is that bilateral agreements like the 2015 Agreement and the Phase One Agreement require voluntary cooperation by both parties. And, given the current state of U.S. China relations, it is unlikely that the U.S. and China can achieve meaningful cooperation in the near term. But beyond the U.S.-China relationship, these agreements are premised on the idea that the parties share a common interest in the ultimate goal. And, somewhat pessimistically, that might not be the case with cyber economic espionage right now.

For the state engaging in economic espionage, the cost is low. Cyber tools are comparatively cheap. There is little chance of criminal or civil punishment from the U.S. Nor is there much chance that the state will receive condemnation from the broader international community. Countries do not agree on the permissibility of economic

---

[165] OFF. OF THE U.S. TRADE REPRESENTATIVE & U.S. DEP'T OF THE TREASURY, ECONOMIC TRADE AGREEMENT BETWEEN THE UNITED STATES OF AMERICA AND THE PEOPLE'S REPUBLIC OF CHINA: PHASE ONE (Jan. 15, 2020) [hereinafter Phase One Agreement], https://ustr.gov/sites/default/files/files/agreements/phase%20one%20agreement/Economic_And_Trade_Agreement_Between_The_United_States_And_China_Text.pdf.

[166] Wendy Wu and Jun Mai, *No time for talking on US-China trade deal in Joe Biden's first 100 days*, SOUTH CHINA MORNING POST (May 1, 2021), https://www.scmp.com/news/china/diplomacy/article/3131721/no-time-talking-us-china-trade-deal-bidens-first-100-days.

espionage.[167] No treaty in international law discusses the use of economic espionage; nor is there a consensus in the international community as to whether any body of customary international law applies.[168] At present, the cyber norms creation process is effectively stalled; the recent report of the UN Open-Ended Working Group (OEWG) on Developments in the Field of Information and Telecommunications in the Context of International Security declined to take a position on whether the law of armed conflict (and thereby the law of countermeasures) applies in cyberspace.[169] Rather, the report simply reiterates that states should seek to solve disputes through peaceful means such as negotiation or mediation.[170] And the pay-off for the state engaging in economic espionage is potentially quite high; for some states, economic espionage represents a meaningful way to facilitate economic development and economic growth.[171]

Because there is such a large gap between the U.S.'s equities and the foreign government's equities it is unlikely–absent revolutions in foreign interests and international law–that bilateral, voluntary agreements will provide a lasting solution for the economic espionage problem. So, while the U.S. should not expect international agreements to meaningfully curb economic espionage in the near-term, it should continue to use diplomatic efforts to advance better normative behavior in the long-term.

---

[167] Reid*, supra* note 22, at 765
[168] S*ee* Lotrionte, *supra* note 26 (discussing potential, but not settled applications of existing international law to cyber economic espionage).
[169] Final Substantive Rep., Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, U.N. Doc. A/AC.290/2021/CRP.2.
[170] *Id*. at 6.
[171] Reid, *supra* note 22, at 765.

E. DEFENDING GOVERNMENT NETWORKS & ENGAGING THE PRIVATE SECTOR

The U.S. government also engages in activities designed to prevent or defend against cyber economic espionage. Richard Clarke and Robert Knake refer to the idea of cyber resilience as "the best bad idea we've got."[172] So long as the U.S. government's policies are insufficient to stop or meaningfully punish economic espionage, Clarke and Knake seem to be correct. The U.S. government's cyber-related defensive activities can be split into two groups–first, the U.S. government protects its own networks; second, the U.S. government engages the private sector to encourage better defense.

It is the federal government's job to protect federal networks. In the aftermath of large-scale intrusions like China's OPM hack in 2015 and Russia's SolarWinds hack earlier this year, it is clear that the federal government must do a *better* job protecting federal networks.[173] Neither of these hacks constitute economic espionage, but the major security failures that gave way to these hacks certainly have implications for economic espionage. Writing for Lawfare, Johnathan Reiber and Matt Glenn explain with regard to the SolarWinds hack–

> Although the United States is the home of many top cybersecurity companies, the U.S. government is behind where it should be both in technology modernization and in mindset. Best-in-class cyberdefense technologies have been available on the market for years, yet the U.S. government has failed to adopt them, opting instead to treat cybersecurity like a counterintelligence problem and focusing most of its resources on detection. Yet the government's massive perimeter detection technology, Einstein, failed to detect the SolarWinds intrusion—which lays bare the inadequacy of this approach.[174]

---

[172] CLARKE, *supra* note 59, at 85.
[173] Jonathan Reiber & Matt Glenn, *The U.S. Government Needs to Overhaul Cybersecurity: Here's How*. LAWFARE (Apr. 9, 2021), https://www.lawfareblog.com/us-government-needs-overhaul-cybersecurity-heres-how.
[174] *Id.*

A perimeter security model protects the outside edges or perimeter of a network; however, once an intruder has made her way inside, perimeter security does nothing to keep her from moving around the network freely. While it may be too expensive to replace the whole system at once, the U.S. government can begin to modernize its defenses by transitioning away from a perimeter security model towards a zero-trust model. A zero-trust model does away with the inside, outside distinction and requires continuous verification when attempting to navigate a network. Ultimately updating the way the U.S. government protects its networks will help prevent economic espionage.

By contrast, it is not the federal government's job to protect private networks.[175] It has neither the capacity nor the authority. So, though private networks account for far more of the attack surface for economic espionage, the government merely plays a supporting role to private sector defense. The U.S. government provides a variety of opportunities for public/private partnership and information sharing about threats, vulnerabilities, and other risks; it provides outlets for reporting and incident response; it provides training and education programs on cybersecurity and information security to private industry; and it provides comprehensive guidance for risk-assessment, best-practices, and capacity development.[176] But the efficacy of these efforts is entirely dependent on private industry's voluntary participation and engagement. At present, private industry is simply not buying-in the way it needs to.[177]

[175] *Id.*
[176] NCSC 2018, *supra* note 24, at 15.
[177] Reid, *supra* note 22, at 802.

There are two big problems when it comes to improving private sector defense–cost and apathy. First, cybersecurity is expensive, and the cost is rising.[178] Accenture's 2020 Cyber Resilience Report shows that, across security components, most companies have seen the cost of cybersecurity rise 25% or more in the last two years. Of the seventeen security components the report accounts for,[179] the largest increases in cost were for network security, threat detection, and security monitoring tools. And while we might not be worried about the ability of industry leaders to bear increasing costs in the near term, we should be worried about the ability of companies further down the supply chain. For many businesses, security costs limit the company's ability to protect their networks properly.

Simply throwing money at security does not work; not all security products are made equal. Companies have to invest in cybersecurity efficiently and strategically. And this is harder than it sounds because the market for cybersecurity products, and for IT more generally, is inefficient. Cybersecurity research and startups are largely funded by venture capital (VC).[180] But because everyone is looking for the next "billion-dollar unicorn," venture "tourists" have flooded the market.[181] The result is that "many of the three thousand cybersecurity companies 'are a feature, not a firm[.]' . . . They solve one narrow problem and really should be part of a platform company offering a mutually

[178] KELLY BISSEL, RYAN M. LASALLE, & PAOLO DAL CIN, INNOVATE FOR CYBER RESILIENCE LESSONS FROM LEADERS TO MASTER CYBERSECURITY EXECUTION 12 (Accenture Security, 2020).
[179] 1. Network security 2. Threat detection 3. Security monitoring 4. Cyber risk management 5. Firewalls 6. Threat intelligence 7. Application security 8. End-point detection and response 9. Incident response 10.Identity and access management 11. Vulnerability management 12.OT-related security 13.Privileged Access Management 14.Staffing (or People) 15.Remediation 16.Governance, Risk, and Compliance 17. SIEM and event consoles *Id.*
[180] CLARKE, *supra* note 59, at 69.
[181] *Id.*

supporting mesh of integrated security products."[182] This market structure impedes innovation, and it precludes efficient security. The concept is not dissimilar to the experience of paying for six different streaming services; none of them have every show you want, and all of them are *just different enough* to make it seem worthwhile. For.cost-limited businesses, this often leads to gaps in network protection or spending money on one security component at the expense of another. A business may purchase the threat detection software and forgo the vulnerability management tool.

Of course, to prevent economic espionage, cybersecurity is not all a company needs; strong cybersecurity must be paired with physical security (like ID badges) and other forms of information security (like tiered classification). Cybersecurity can protect a company from unauthorized cyber-enabled theft, but of course, not all economic espionage is cyber-enabled. Nor is all economic espionage committed by unauthorized persons–insiders pose a huge threat to trade secrecy. And these security tools are going to carry their own, additional costs.

The second, and perhaps more damning problem, is apathy. Companies have long been rather ambivalent when it comes to the threat of economic espionage; "[a]mongst the general public there exists the perception that economic espionage is not a pressing problem, but rather an inevitable consequence of globalization."[183] But at what point does cyber economic espionage become a pressing problem for a business? Is it when the trade secrets are stolen? Or when the business realizes the trade secrets

[182] *Id.*
[183] Mark E. Danielson, *Economic Espionage: A Framework for a Workable Solution*, 10 Minn. J.L. Sci. & Tech. 503, 512 (2009).

are stolen? Or when a competitive good appears on the market? At any of these points, it is already too late for defense.

And It is clear that private industry does not *want* greater government intervention in this space. As explained by Clarke and Knake,

> [c]yber resilience, prioritizing network defense and making the private sector bear the cost of absorbing these attacks is, at first blush, an unappealing prospect to most CEOs . . . .Yet every time policy makers unpack how the government could take on this responsibility, private sector enthusiasm quickly begins to fade because of the unintended consequences of government involvement. On cybersecurity, there are only bad options. Private responsibility for network defense with government support is the least bad one.[184]

There have been attempts to introduce regulation in the past that would mandate security standards for critical infrastructure, but, unsurprisingly, industry was unsupportive.[185] The private sector does not want to pay the compliance costs that would accompany regulation in this space. However–the longer it takes for businesses to recognize the severity of the problem, the greater the chance becomes that the federal government will choose to regulate. And the longer it takes the federal government to regulate the greater the chance becomes that the *states* will choose to regulate, individually.[186] If U.S. businesses really want to avoid compliance costs in the long run, it is in their best interest to properly defend against the problem now. For its part, the U.S. government must do what it can to make cybersecurity more accessible and affordable for U.S. businesses.

---

[184] *Id.* at 105.
[185] CLARKE, *supra* note 59, at 109.
[186] *Id.* at 107.

V. ADDRESSING THE PROBLEM

Cyber economic espionage threatens American businesses, and it threatens American national security. At the cost of hundreds of millions of dollars per year and millions of jobs, cyber economic espionage cannot be treated as just another cost of doing business in the digital age. Addressing the problem requires a robust response from both the U.S. government and U.S. businesses.

In his first address to Congress, President Biden stated, "America will stand up to unfair trade practices that undercut American workers and American industries, like subsidies to state-owned enterprises and the theft of American technology and intellectual property."[187] The necessary question is–how? So far, rare prosecutions, speaking indictments, civil suits, trade tariffs, and bilateral agreements seem insufficient to curb the problem. And, in order to prevent theft, defense of both of government and private networks must be improved.

The following recommendations aim to improve both the U.S. reaction to and defense against cyber economic espionage.

Increase Awareness of the threat posed by state-sponsored theft of trade secrets in order to encourage the private sector and the international community to take on more responsibility in addressing the threat.

- The U.S. government should strive to increase private sector awareness of the threat through regular reporting on state actor threats and methods. This should
- The U.S. government should strive to increase recognition of the threat in the international community. As suggested in the 2021 Update from the IP

[187] *Remarks as Prepared for Delivery by President Biden–Address to a Joint Session of Congress*, THE WHITE HOUSE (Apr. 28, 2021), https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/04/28/remarks-as-prepared-for-delivery-by-president-biden-address-to-a-joint-session-of-congress/.

Commission, the U.S. should create a multinational registry to share information on bad actors.[188]
- The U.S. government should use its standing in international fora to advance norms creation on the issue of state sponsored theft of trade secrets; and it must take particular care to articulate why economic espionage, as an act of theft, differs from other unfair economic practices.
- The U.S. government should continue to engage adversarial governments through diplomatic means to encourage better normative behavior in the long run.

Increase Reporting in order to better understand the full scope and scale of the problem. Ultimately, having a better understanding of the threat will allow for more effective resource and response allocation.

- The U.S. government should mandate reporting of theft of trade secrets and proprietary information relating to critical infrastructure and critical technologies such as those regulated by export controls.
- The U.S. government should take an incentive-based approach to increase reporting for other industries.
- The U.S. government must provide additional assurances regarding protection from further disclosure of trade secrets in order to address the privacy concerns of victim companies.

Modernize Defense of Federal Networks in order to better protect against economic espionage and other malicious intrusions.

- The U.S. government must immediately work to design and implement a continuously validated zero-trust architecture to protect the federal government's most critical assets.[189]
- The U.S. government should invest in end-point detection and segment its networks in order to ensure a compromised device cannot compromise other devices on the network.

Promote Private Responsibility

[188] DENNIS C. BLAIR & JON M. HUNTSMAN, JR., IP COMMISSION 2021 REVIEW: UPDATED RECOMMENDATIONS 2 (2021).
[189] Reiber, *supra* note 173.

- U.S. businesses must do more to defend against the threat of cyber economic espionage. Most immediately, companies can help curb the impact of economic espionage by practicing good cyber hygiene and adopting robust trade secrecy programs.
- U.S. businesses must adopt comprehensive cybersecurity must be paired with physical security and good information governance. strong information security or trade secret governance. Cybersecurity can help defend against unauthorized, cyber-enabled attacks. A strong trade secret policy can help keep secrets safe regardless of the method the thief is using to try to obtain them.

Provide Incentives to the private sector in order to encourage better defense.

- The U.S. government should establish an incentive program, such as a tax credit or subsidy, for companies that adopt and maintain set security standards. This program would make spending on cybersecurity more attractive. And for companies that are otherwise cost-limited, this program would make cybersecurity more accessible.

BIBLIOGRAPHY

STATUTES & REGULATIONS

18 U.S.C. § 1030 (2020).

18 U.S.C. § 1341 (2008).

18 U.S.C. § 1343 (2008).

18 U.S.C. § 1346 (1988).

18 U.S.C. § 1831 (2012).

18 U.S.C. § 1832 (2016).

18 U.S.C. § 1836 (2016).

18 U.S.C. § 1956 (2016).

18 U.S.C. § 1957 (2012).

18 U.S.C. § 2314 (2013).

22 U.S.C. § 2778 (2014).

22 C.F.R. § 120 (2014).

32 C.F.R. § 236 (2016).

CASES

United States v. Hanjuan Jin,
773 F.3d 718, 720 (7th Cir. 2013).

U.S. v. Lan Lee,
No. CR 06-0424 JW, 2010 WL 8696087 (N.D. Cal. 2010).

U.S. v. Hanjuan Jin,
833 F.Supp.2d 977 (N.D. Ill. 2012), aff'd, 733 F.3d 718 (7th Cir. 2013).

vPersonalize Inc. v. Magnetize Consultants Ltd.,
No. 2:18-CV-01836-BJR, 2020 WL 534505 (W.D. Wash. Feb. 3, 2020).

ADDITIONAL SOURCES

Adam Segal, *The U.S.-China Cyber Espionage Deal One Year Later*, COUNCIL ON FOREIGN REL. (Sep. 28, 2016), https://www.cfr.org/blog/us-china-cyber-espionage-deal-one-year-later.

Catherine Lotrionte, *Countering State-Sponsored Cyber Economic Espionage Under International Law*, 40 N.C.J. Int'l L. & Com. Reg. 443 (2015).

Chad P. Bown, *U.S. China Trade War Tariffs: An Up-to-Date Chart*, PETERSON INST. FOR INT'L ECON. (Mar. 16, 2021), https://www.piie.com/research/piie-charts/us-china-trade-war-tariffs-date-chart.

Charles R. Morris, *We Were Pirates, Too*, FOREIGN POL'Y (Dec. 6, 2012), https://foreignpolicy.com/2012/12/06/we-were-pirates-too/.

CONG. RES. SERV., INTELLECTUAL PROPERTY VIOLATIONS AND CHINA: LEGAL REMEDIES 1 (2020).

CONG. RES. SERV., SECT. 301 OF THE TRADE ACT OF 1974 1 (2021) [hereinafter CRS Trade Act Analysis].

CTR. FOR STRATEGIC INT'L STUD., THE ECONOMIC IMPACT OF CYBERCRIME–NO SLOWING DOWN 8 (2018), https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf.

Danielle A. Duszczysyn & Daniel F. Roland, *Three Years Later: How the Defend Trade Secrets Act Complicated the Law Instead of Making it More Uniform* FINNEGAN (Jul. 2019), https://www.finnegan.com/en/insights/articles/three-years-later-how-the-defend-trade-secrets-act-complicated-the-law-instead-of-making-it-more-uniform.html.

David E. Sanger & Steven Lee Myers, *After a Hiatus, China Accelerates Cyberspying Efforts to Obtain U.S. Technology*, N.Y. TIMES (Nov. 29, 2018), https://www.nytimes.com/2018/11/29/us/politics/china-trump-cyberespionage.html.

DAVID E. SANGER, THE PERFECT WEAPON: WAR SABOTAGE, AND FEAR IN THE CYBER AGE 120 (Crown 2018).

David Hechler, *What is the Point of These Nation-State Indictments?* LAWFARE (Feb. 8, 2021), https://www.lawfareblog.com/what-point-these-nation-state-indictments.

DENNIS C. BLAIR & JON M. HUNTSMAN, JR., THE IP COMMISSION REPORT: THE REPORT OF THE COMMISSION ON THE THEFT OF AMERICAN INTELLECTUAL PROPERTY (2013).

DENNIS C. BLAIR & JON M. HUNTSMAN, JR., UPDATE TO THE IP COMMISSION REPORT: THE THEFT OF AMERICAN INTELLECTUAL PROPERTY REASSESSMENTS OF THE CHALLENGE AND UNITED STATES POLICY (2017).

DENNIS C. BLAIR & JON M. HUNTSMAN, JR., IP COMMISSION 2021 REVIEW: UPDATED RECOMMENDATIONS (2021).

Derek B. Johnson, *DOJ official says 'name and shame' is one piece of the puzzle*, FWC (Jan. 18, 2019), https://fcw.com/articles/2019/01/18/demers-doj-cyber-shame.aspx.

DIEI FLORENCIO & CORMAC HERLEY, SEX LIES AND CYBER-CRIME SURVEYS (Microsoft Research, 2011).

DOUGLAS THOMAS, DEP'T OF COMM. NAT'L INST. OF STANDARDS AND TECH., MAN. SER. 100-32, CYBERCRIME LOSSES: AN EXAMINATION OF U.S. MANUFACTURING AND THE TOTAL ECONOMY (2020) [hereinafter NIST Report] https://nvlpubs.nist.gov/nistpubs/ams/NIST.AMS.100-32.pdf.

Economic Espionage Act of 1996, Publ. L. 104-294, § 1836, 110 Stat. 3488, 3490 (1996).

ECONOMICS & STATISTICS ADMINISTRATION & U.S. PATENT AND TRADEMARK OFFICE, INTELLECTUAL PROPERTY AND THE U.S. ECONOMY: 2016 UPDATE (2016), https://www.uspto.gov/sites/default/files/documents/IPandtheUSEconomySept2016.pdf.

Final Substantive Rep., Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, U.N. Doc. A/AC.290/2021/CRP.2.

Flora Lewis, "Soviets Buy American," NEW YORK TIMES (May 10, 1989), https://www.nytimes.com/1989/05/10/opinion/foreign-affairs-soviets-buy-american.html.

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

Franz-Stefan Gady, "New Snowden Documents Reveal Chinese Behind F-35 Hack," THE DIPLOMAT (Jan. 27, 2015), https://thediplomat.com/2015/01/new-snowden-documents-reveal-chinese-behind-f-35-hack/.

Garret Hinck & Tim Maurer, *What's the Point of Charging Foreign State-Linked Hackers?*, LAWFARE (May 24, 2019), https://www.lawfareblog.com/whats-point-charging-foreign-state-linked-hackers.

H.R. 3723 (104TH): ECONOMIC ESPIONAGE ACT OF 1996, https://www.govtrack.us/congress/bills/104/hr3723;

Information About the Department Of Justice's China Initiative and A Compilation of China-Related Prosecutions Since 2018, U.S. DEPT. OF JUST. (last visited Mar. 13, 2021), https://www.justice.gov/nsd/information-about-department-justice-s-china-initiative-and-compilation-china-related.

Jack Goldsmith, *The Puzzle of the GRU Indictment*, LAWFARE (Oct. 21, 2020), https://www.lawfareblog.com/puzzle-gru-indictment.

James M. Fischer, *Note: An Analysis of Economic Espionage Act of 1996*, 25 SETON HALL LEGIS. J. 239, (2001).

Jeremy S. Wu, "Federal Cases," JEREMY S. WU, PHD (Last visited Apr. 23, 2021) https://jeremy-wu.info/fed-cases/ [hereinafter Federal Cases].

Jonathan Reiber & Matt Glenn, *The U.S. Government Needs to Overhaul Cybersecurity: Here's How*. LAWFARE (Apr. 9, 2021), https://www.lawfareblog.com/us-government-needs-overhaul-cybersecurity-heres-how.

JOSH ROGIN, CHAOS UNDER HEAVEN: TRUMP, XI, AND THE BATTLE FOR THE 21ST CENTURY 146 (Houghton Mifflin Harcourt, 2021).

KELLY BISSEL, RYAN M. LASALLE, & PAOLO DAL CIN, INNOVATE FOR CYBER RESILIENCE LESSONS FROM LEADERS TO MASTER CYBERSECURITY EXECUTION (Accenture Security, 2020).

Mark E. Danielson, *Economic Espionage: A Framework for a Workable Solution*, 10 Minn. J.L. Sci. & Tech. 503, 512 (2009).

MARK M. LOWENTHAL, INTELLIGENCE: FROM SECRETS TO POLICY 489 (7th ed. 2017).

Melanie Reid, *A Comparative Approach to Economic Espionage: Is Any Nation Effectively Dealing With This Global Threat?*, 70 U. MIAMI L. REV. 757 (2016) (discussing how different countries approach economic espionage).

Michelle Van Cleave, Nat'l Counterintelligence Executive, Remarks at the Conference on Counterintelligence for the 21st Century: The National Counterintelligence Strategy of the U.S. (Mar. 4–5, 2005), https://fas.org/irp/news/2005/03/ncix030505.pdf.

NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER, FOREIGN ECONOMIC ESPIONAGE IN CYBERSPACE (2018).

NICOLE PERLROTH, THIS IS HOW THEY TELL ME THE WORLD ENDS: THE CYBER-WEAPONS ARMS RACE (Bloomsbury Publishing, 2021).

OFF. OF THE DIRECTOR OF NATIONAL INTELLIGENCE, ANNUAL THREAT ASSESSMENT OF THE U.S. INTELLIGENCE COMMUNITY (2021).

OFF. OF THE NAT'L COUNTERINTELLIGENCE EXECUTIVE, ANNUAL REPORT TO CONGRESS ON FOREIGN ECONOMIC COLLECTION AND INDUSTRIAL ESPIONAGE: 1996 (1996).

OFF. OF THE U.S. TRADE REPRESENTATIVE & U.S. DEP'T OF THE TREASURY, ECONOMIC TRADE AGREEMENT BETWEEN THE UNITED STATES OF AMERICA AND THE PEOPLE'S REPUBLIC OF CHINA: PHASE ONE (Jan. 15, 2020), https://ustr.gov/sites/default/files/files/agreements/phase%20one%20agreement/Economic_And_Trade_Agreement_Between_The_United_States_And_China_Text.pdf.

Ph.D. Chemist Convicted Of Conspiracy To Commit Economic Espionage, Theft Of Trade Secrets, And Wire Fraud, U.S. DEPT. OF JUST. (last visited Apr. 24, 2021), https://www.justice.gov/usao-edtn/pr/phd-chemist-convicted-conspiracy-commit-economic-espionage-theft-trade-secrets-and-wire.

President Barack Obama, Remarks by President Obama and President Xi of the People's Republic of China in Joint Press Conference (Sep. 25, 2015), https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/remarks-president-obama-and-president-xi-peoples-republic-china-joint.

President William Clinton, Statement on Signing the Economic Espionage Act of 1996 (Oct. 11, 1996), https://www.govinfo.gov/content/pkg/WCPD-1996-10-14/pdf/WCPD-1996-10-14-Pg2040-2.pdf.

Prosecuting Chinese "Spies": An Empirical Analysis of the Economic Espionage Act, 40 CARDOZO LAW REVIEW 751 (2018).

Rajesh Kumar Singh, *Explainer: Trump's China tariffs - Paid by U.S. importers, not by China*, REUTERS (Aug. 1, 2019), https://www.reuters.com/article/us-usa-trade-china-tariffs-explainer/explainer-trumps-china-tariffs-paid-by-u-s-importers-not-by-china-idUSKCN1UR5YZ.

Remarks as Prepared for Delivery by President Biden–Address to a Joint Session of Congress, THE WHITE HOUSE (Apr. 28, 2021), https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/04/28/remarks-as-prepared-for-delivery-by-president-biden-address-to-a-joint-session-of-congress/.

RICHARD A. CLARKE & ROBERT K. KNAKE, THE FIFTH DOMAIN: DEFENDING OUR COUNTRY, OUR COMPANIES, AND OURSELVES IN THE AGE OF CYBER THREATS (Penguin Press, 2019).

Robin L. Kuntz, *How Not to Catch a Thief: Why the Economic Espionage Act Fails to Protect American Trade Secrets*, 28 BERKELEY TECH. L.J. 901 (2013).

S. Rep. No. 105-1.

SUSAN RICE, TOUGH LOVE: MY STORY OF THE THINGS WORTH FIGHTING FOR (Simon & Schuster, 2019).

Susan W. Brenner & Anthony C. Crescenzi, *State-Sponsored Crime: The Futility of the Economic Espionage Act*, 28 HOUS. J. INT'L L. 389 (2006).

Taiwan Company Pleads Guilty to Trade Secret Theft in Criminal Case Involving PRC State-Owned Company, U.S. DEPT. OF JUST. (last visited Apr. 24, 2021), https://www.justice.gov/usao-ndca/pr/taiwan-company-pleads-guilty-trade-secret-theft-criminal-case-involving-prc-state-owned.

THE WHITE HOUSE OFFICE OF THE PRESS SECRETARY, FACT SHEET: PRESIDENT XI JINPING'S STATE VISIT THE UNITED STATES (2015), https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states .

THOMAS RID, CYBER WAR WILL NOT TAKE PLACE (Oxford University Press, 2013).

U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage, U.S. DEPT. OF JUST. (last visited Feb. 8, 2021) https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

Wendy Wu and Jun Mai, *No time for talking on US-China trade deal in Joe Biden's first 100 days*, SOUTH CHINA MORNING POST (May 1, 2021), https://www.scmp.com/news/china/diplomacy/article/3131721/no-time-talking-us-china-trade-deal-bidens-first-100-days.

What is "economic espionage"?, DEP'T OF JUST. FED. BUREAU OF INVESTIGATION (last visited Feb. 6, 2021), https://www.fbi.gov/about/faqs/what-is-economic-espionage.