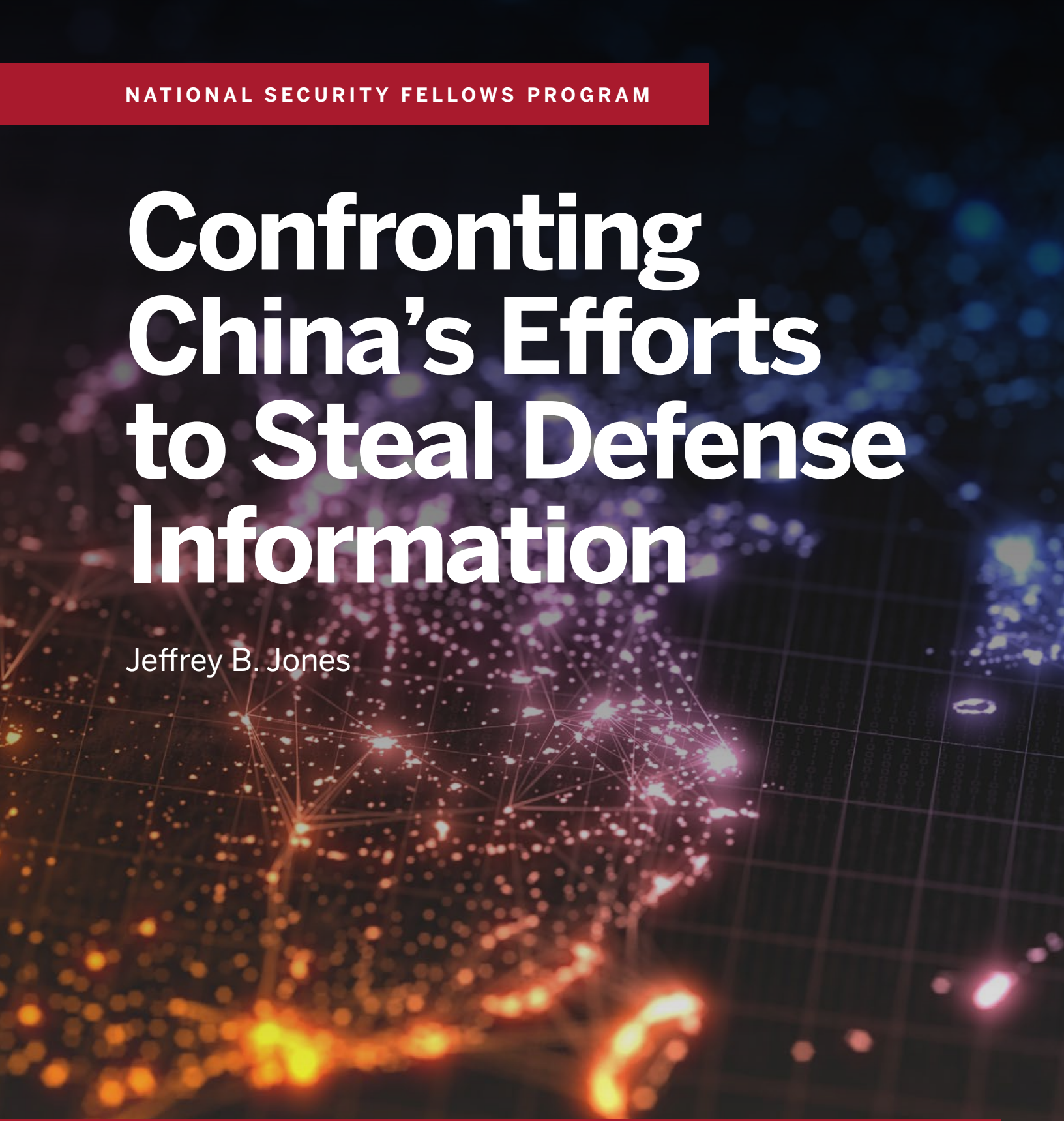
NATIONAL SECURITY FELLOWS PROGRAM

# Confronting China's Efforts to Steal Defense Information

Jeffrey B. Jones



HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

PAPER
MAY 2020

**National Security Fellowship Program**
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 JFK Street
Cambridge, MA 02138

**www.belfercenter.org/NSF**



Design and layout by Andrew Facini


Printed in the United States of America

NATIONAL SECURITY FELLOWS PROGRAM

# Confronting China's Efforts to Steal Defense Information

Jeffrey B. Jones

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

PAPER
MAY 2020

# Acknowledgments

Foremost, I thank my wife, Charlene, and my son, Jake, for providing me with the encouragement and support to conduct research that will hopefully inspire others to make America a safer and more secure place for people to pursue their dreams. I would also like to express my sincere appreciation to my Army War College advisor, Megan Hennessey, Ph.D., for her input, advice and assurance throughout the research and drafting process. Furthermore, I would like to acknowledge MG(Ret) William Rapp, Jim Waldo, Bruce Schneier, Raymond Yom, Phil Evans, Sean Clougherty and Eric Rosenbach for their contributions, both big and small, to this project. Finally, I extend my gratitude and thanks to the entire 2019-2020 Harvard National Security Fellowship cohort for setting an example of excellence and professionalism that I will continually strive to emulate.

# About the Author

Lieutenant Colonel (LTC) Jeffrey Jones is an Army Reserve Judge Advocate General. As a civilian, LTC Jones serves as the Senior Legal Advisor for a Major Subordinate Command belonging to the U.S. Army Intelligence and Security Command. Previously, he served as a Prosecutor for the Office of Military Commissions, as well as a Soldier's Counsel at Walter Reed Army Medical Center. He has also held positions as a Prosecutor for Immigration and Customs Enforcement (ICE), a Legal Advisor for ICE's National Security Law Division, and an Attorney Advisor for the U.S. Department of Justice in its National Security Division. LTC Jones is a graduate of the Defense Language Institute's Basic Arabic language course and holds a bachelor's degree in Government and Politics from the University of Maryland at College Park and a juris doctorate from the University of Maryland.

# Table of Contents

# 1. Introduction

China's cyber espionage activities[1] represent a significant threat to the United States military and the safety and security of this nation. Defense contractors, research institutes, and universities are failing to adequately secure their computer networks, allowing China to steal research and development pertaining to some of America's most important military technology. This wholesale theft represents losses to the United States in the range of hundreds of billions of dollars per year.[2]

So, why are contractors and research institutes so vulnerable to having their work product stolen? Given the technical and sensitive nature of these activities one would assume that these companies would take enormous care in protecting that information from being stolen or destroyed. What, after all, could be more important than information pertaining to the defense of the nation? However, the track record for many defense contractors in protecting classified information is abysmal and seems to suggest that the United States government values this information much more than the companies contracted to research and develop it. Simply put, the United States is not incentivizing the protection of this information, so contractors and research institutes are not making cybersecurity a priority.

Considering this deeply troubling reality, the United States government must require private industry and research institutions to take this threat seriously and develop cybersecurity policy and practices that will result in multiple layers of cybersecurity protections. This layered approach will require combined efforts from both the government and private industry to create an overlapping protection scheme. This method should support a resilient cyber defense posture that can still be effective in the event individual components of the strategy fail. The

1 For the purposes of this paper, "cyber espionage" is defined as the unauthorized access of a network in order to steal national security information to aid foreign governments. This definition blends the concepts of "cyber espionage", "cyber crime" and "cyber-enabled economic warfare" but is being used in this context as a shorthand to describe China's theft of intellectual property. Samantha F. Ravich and Annie Fixler, "Framework and Terminology for Understanding Cyber-Enabled Economic Warfare," n.d., 6.

2 Zack Cooper, "Understanding the Chinese Communist Party's Approach to Cyber-Enabled Economic Warfare," September 2018, 21.

approach must introduce a comprehensive array of obstacles and deterrents that could help prevent China from having the nearly unrestricted access it currently seems to enjoy to this information. A crucial component to this strategy is incentivizing these companies and research institutes to value this information as much as the government does. If the government is paying for the research and development, it is only reasonable to assume that this payment agreement includes the assurance that the work product will be protected from theft. This approach will result in a cybersecurity model that recognizes the value of a defense-in-depth approach and eliminates any notion that a single solution can prevent the Chinese from stealing the Department of Defense's (DOD's) most valuable intellectual property.[3]

## 2. Understanding the Problem

Espionage, in one form or another, is a common nation-state activity that has existed for thousands of years.[4] The United States conducts espionage against other nations to furnish its military and political decision makers with the necessary information to inform policy, influence military readiness, and positively impact military outcomes. The United States considers espionage as a nation-state activity conducted solely for the benefit of government decision makers to understand the capabilities, intentions and activities of potential adversaries and to protect the security interests of the United States. On the other hand, while China engages in espionage to inform its decision makers, it also shares the information it collects with Chinese companies. This policy amounts to nothing more than Chinese-sponsored corporate theft, which China is using to feed its long-term economic and military future. To determine what China is focused on procuring, one need look no further than China's "Made in China 2025" strategy - a decade-long plan wherein it identifies ten industries it is

3 "Defense Industrial Base Sector," Department of Homeland Security, June 12, 2014, https://www.dhs.gov/cisa/defense-industrial-base-sector. This paper will refer to DOD intellectual property, however, that term is meant to refer to the research and development efforts of the more than 100,000 companies and subcontractors that collectively comprise what the Department of Homeland Security identifies as the "Defense Intelligence Base" (DIB).

4 Darien Pun, "Rethinking Espionage in the Modern Era," *Chicago Journal of International Law* 18, no. 1 (n.d.): 355.

targeting to dominate in the future and which serves as a "roadmap" to the theft in which China is engaging.[5] The industries identified in this strategy either directly or indirectly impact the United States' ability to wage, or defend against, military action against its adversaries.

The monetary value of the information China is stealing is astounding. Chinese intellectual property theft is costing industry in the range of $180 billion to as high as $540 billion per year.[6] The cost estimates can vary significantly from one another because much of the value of this information tends to be intrinsic. Some of the factors used in estimating cost include reputational damage, regulatory penalties, and the loss of strategic information and intellectual property advantages.[7] These estimates represent espionage-related theft in both the cyber and physical domains. In November 2015, the Office of the Director of National Intelligence (ODNI) refined those figures and estimated that the United States is losing approximately $400 billion annually to thefts occurring in the cyber domain.[8] According to a 2013 report from Verizon, China is responsible for more than 90 percent of known cyber espionage activities in the United States.[9] In the wake of a 2015 United States-China Cyber Agreement, FireEye, a cybersecurity company, determined that the frequency of Chinese-related cyber intrusions tumbled by nearly 90 percent by the middle of 2016 in the wake of a Chinese-United States agreement on cyber espionage.[10]

5 "John C. Demers, Assistant Attorney General, National Security Division, Department of Justice, Statement before the Senate Committee on the Judiciary, 'China's Non-Traditional Espionage Against the United States, The Threat and Potential Policy Responses,'" December 12, 2018, 1–2.

6 "IP_Commission_Report_Update_2017.Pdf," 12, accessed August 24, 2019, http://www.ipcommission.org/report/IP_Commission_Report_Update_2017.pdf.

7 "The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.Pdf," 6, accessed November 24, 2019, https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf. One other component of the cost assessment that may or may not end up in cost estimates include the extreme costs associated with the research and development of the information that China is able to avoid spending as a result its illicit behavior.

8 "No Sign China Has Stopped Hacking U.S. Companies, Official Says - Bloomberg," accessed September 2, 2019, https://www.bloomberg.com/news/articles/2015-11-18/no-sign-china-has-stopped-hacking-u-s-companies-official-says.

9 Zack Cooper, "Understanding the Chinese Communist Party's Approach to Cyber-Enabled Economic Warfare," September 2018, 6.

10 "Rpt-China-Espionage.Pdf," 11, accessed September 2, 2019, https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf.

Unfortunately, the United States assesses that the rate of Chinese cyber espionage activity has rebounded to its pre-agreement levels.[11]

The extent of Chinese cyber espionage activities is likely significantly more serious than what news organizations and industry representatives are revealing. Given the clandestine nature of cyber espionage, some cyber intrusions may simply go undetected. Furthermore, the damage a cyber intrusion can cause to an organization's reputation and its public standing often prevents companies from disclosing that a breach occurred. The threat that such a revelation may pose to a company's ability to compete for future business may influence these organizations to simply remain quiet.[12] Additionally, industry lacks the confidence that law enforcement has the capacity or the wherewithal to effectively respond to a breach.[13] If an organization was convinced that the government was capable of retrieving the stolen information, or even deleting the information from the thief's computer system, it may be incentivized to report the breach and ignore the potential cost such a report could represent to future business.

The Federal Government may choose not to publicly disclose a breach out of a concern that such a report may jeopardize the sources and methods it used to determine that the adversary breached the system. There is also some intelligence value to the government allowing a breach to unfold and learning how the adversary operates in the breached system. This overwatch technique can allow technicians to pinpoint system flaws and aid them in developing countermeasures to prevent a similar exploit from occurring in the future.

Clearly, under-reporting creates a problem for policy makers in gaining a firm understanding of the full extent of the problem. Nonetheless, a

11 "U.S.' Top Spy-Catcher: China Brings 'Ungodly Resources' to Espionage - CBS News," accessed September 2, 2019, https://www.cbsnews.com/news/ncsc-director-says-china-is-the-largest-threat-to-national-security/. FireEye and the Department of Justice assess the decline between 2013 to 2016 may have been attributed to the Chinese refining their tactics and techniques. This rebound may simply reflect the United States' increased ability to detect and identify these intrusions. See also "The U.S.-China Cyber Espionage Deal One Year Later | Council on Foreign Relations," accessed September 2, 2019, https://www.cfr.org/blog/us-china-cyber-espionage-deal-one-year-later.

12 "The Real Reasons Why Cybercrimes Are Vastly Underreported.," accessed September 2, 2019, https://slate.com/technology/2018/02/the-real-reasons-why-cybercrimes-are-vastly-underreported.html.

13 "The Real Reasons Why Cybercrimes Are Vastly Underreported."

conservative approach that takes into account all aspects of the previous discussion yields an estimated loss of approximately $300 billion per year to Chinese cyber espionage activities.[14] The sheer magnitude of the value of the theft is alarming; however, the Chinese government is compounding the severity of the problem by releasing the results of this corporate theft to leading Chinese companies so that they can accelerate their research and development efforts without having to spend any money or devote the massive amounts of time and resources necessary to arrive at the information on their own.

The Chinese Communist Party (CCP) exerts control over virtually every aspect of the Chinese economy and views the economy as an extension of the state.[15] Eighty-five percent of the 109 Chinese companies on the Fortune Global 500 list are State Owned Enterprises (SOEs).[16] In 2015, Curtis Milhaupt and Wentong Zheng conducted a review of publicly available information and made the following determination: "Ninety-five out of the top one hundred private firms and eight out of the top ten Internet firms whose founder or de facto controller is currently or formerly a member of central or local party-state organizations."[17] Even if a Privately Owned Entity (POE) in China is not overtly owned and operated by the CCP, it is often heavily influenced by the CCP through the use of incentives and controls, such as subsidies, preferential business treatment and access to government decision makers.[18]

The CCP adheres to a philosophy that every component of Chinese society is responsible for ensuring the national security of the country.[19] This

14 To place this figure in perspective, on March 11, 2019, President Trump proposed to spend $718 billion dollars to cover the costs of running the entire DOD in fiscal year 2020"DOD Releases Fiscal Year 2020 Budget Proposal, U.S. Department of Defense Release," accessed September 2, 2019, https://www.defense.gov/Newsroom/Releases/Release/Article/1782623/dod-releases-fiscal-year-2020-budget-proposal/.

15 Richard McGregor, "How the State Runs Business in China," *The Guardian*, July 25, 2019, sec. World news, https://www.theguardian.com/world/2019/jul/25/china-business-xi-jinping-communist-party-state-private-enterprise-huawei.

16 "Explained, the Role of China's State-Owned Companies," World Economic Forum, accessed October 4, 2019, https://www.weforum.org/agenda/2019/05/why-chinas-state-owned-companies-still-have-a-key-role-to-play/.

17 Curtis J. Milhaupt and Wentong Zheng, "Beyond Ownership: State Capitalism and the Chinese Firm," *The Georgetown Law Journal*, 103 (March 2015): 684.

18 Robert D. Williams, "The 'China, Inc.+' Challenge to Cyberspace Norms.Pdf," 3–4, accessed October 5, 2019, https://www.hoover.org/sites/default/files/research/docs/williams_webreadypdf1.pdf.

19 Williams, "The 'China, Inc.+' Challenge to Cyberspace Norms.Pdf," 5–6.

paradigm essentially makes every Chinese person, company, and institution nothing more than an extension of the CCP. Article 7 of China's 2017 National Intelligence Law states: "Any organization or citizen shall support, assist and cooperate with the state intelligence work in accordance with the law."[20] This prescriptive language represents an expansive interpretation of the role Chinese society plays in the state's business. This cooperative approach provides the CCP with justification for sharing the fruits of its cyber espionage efforts with its SOEs and POEs. This close collaboration between the state and its industries is anathema in the West, but an aspect of Chinese cyber espionage activities that creates a clear danger to the United States. Since China is dedicating the vast resources of its government to steal information, the United States must be prepared to confront the threat with the knowledge that the Chinese government is funding this theft. This significant resource advantage for the Chinese places United States contractors at a considerable disadvantage in preventing this theft on their own.

A 2015 United States-China Cyber Agreement contained a commitment by both countries that neither would "knowingly support cyber-enabled theft of intellectual property...with the intent of providing competitive advantages to companies or commercial sectors."[21] The agreement resulted in an immediate reduction in the number of cyber intrusions attributed to China, but the number of cyber intrusions attributed to China has since rebounded.[22] This may be due to the United States taking a more aggressive stance in cyberspace. Publicly available data covering the last few years indicates that the United States may have dramatically increased the number of cyber attacks against China.[23] Furthermore, the United States'

20 "2017_PRC_NationalIntelligenceLaw.Pdf," accessed October 5, 2019, http://cs.brown.edu/courses/csci1800/sources/2017_PRC_NationalIntelligenceLaw.pdf.

21 "FACT SHEET: President Xi Jinping's State Visit to the United States," whitehouse.gov, September 25, 2015, https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.

22 "After a Hiatus, China Accelerates Cyberspying Efforts to Obtain U.S. Technology." *The New York Times*. Accessed September 1, 2019, https://www.nytimes.com/2018/11/29/us/politics/china-trump-cyberespionage.html.

23 "New CNCERT Report Shows Most Cyber Attacks on China Originate from United States," CPO Magazine, June 24, 2019, https://www.cpomagazine.com/cyber-security/new-cncert-report-shows-most-cyber-attacks-on-china-originate-from-united-states/.

hostile economic policies toward China may have caused China to reassess its interests in abiding by the terms of the Cyber Agreement.[24]

Based on open source reporting, China is not only stealing sensitive defense information, but it is sharing the information with its defense industry to incorporate the research and development into China's next generation of weapons platforms. This symbiotic relationship is allowing China to develop clones of some of the United States' most critical weapons systems, including Lockheed Martin's F-22 Raptor and F-35 Joint Strike Fighters.[25][26] The United States Secretary of Defense, Mark Esper, characterizes China's intellectual property theft as "the greatest intellectual property theft in human history."[27]

China's J-20 fighter appears to be a carbon-copy of America's F-22 fighter jet.[28] Fortunately, the J-20 does not match the F-22's capabilities - yet. The United States assesses that, due to some design flaws and China's sub-standard stealth coating, the stealthy profile of the J-20 is no match for the now-cancelled F-22 program.[29] Likewise, the design of the J-31 tries to emulate the capabilities of the F-35 Joint Strike Fighter. The J-31's design is strikingly similar to that of the F-35 and the F-22.[30] However, just like the J-20, the J-31 is not as stealthy nor capable as its American counterparts.[31] Moreover, there is a belief that China is having difficulty incorporating the stolen information into a unified platform that is capable of performing at the level of the F-35.[32] With more testing and experimentation, however, the Chinese are likely to be able to continue to develop that capability.

24 "A New Old Threat: Countering the Return of Chinese Industrial Cyber Espionage," accessed September 2, 2019, https://www.cfr.org/report/threat-chinese-espionage.

25 Justin Ling, "Man Who Sold F-35 Secrets to China Pleads Guilty," *Vice* (blog), March 24, 2016, https://www.vice.com/en_us/article/kz9xgn/man-who-sold-f-35-secrets-to-china-pleads-guilty.

26 "China Knows All About the F-35 and F-22 (Thanks to the Data It Stole)," June 10, 2019, accessed September 4, 2019, https://nationalinterest.org/blog/buzz/china-knows-all-about-f-35-and-f-22-thanks-data-it-stole-61912.

27 Ellen Ioanes, "China Steals US Designs for New Weapons, and It's Getting Away with 'the Greatest Intellectual Property Theft in Human History,'" Business Insider, accessed October 19, 2019, https://www.businessinsider.com/esper-warning-china-intellectual-property-theft-greatest-in-history-2019-9.

28 Alex Hollings, "Counterfeit Air Power: Meet China's Copycat Air Force," Popular Mechanics, September 19, 2018, https://www.popularmechanics.com/military/aviation/g23303922/china-copycat-air-force/.

29 Hollings.

30 Hollings.

31 Hollings.

32 Hollings.

Both Chinese fighter jet platforms were built using stolen information procured by a Chinese national named Su Bin.[33] On March 23, 2016, Su Bin pleaded guilty in Federal court to gaining unauthorized access to computer networks in the United States to procure military information pertaining to the C-17, F-22, and F35 and giving it to the Chinese government.[34] Su utilized two unidentified co-conspirators to break-in to computer networks who sent Su a list of files and directories to which the co-conspirators had access.[3536] From those lists, Su identified the information that he wanted and the co-conspirators procured the information and sent it to Su - who subsequently translated the information and sent reports addressed to the Second Department, General Staff Headquarters, Chinese People's Liberation Army.[37] It is believed that Su was responsible for stealing 220 megabytes of data pertaining to the F-22 and flight testing information for the F-35.[38]

The Su Bin prosecution represents a victory for the United States in sidelining a prolific cyber espionage actor who posed a significant risk to American military dominance. However, the figures referenced herein establish that this is a problem represented by much more than just one or two actors. This is a concerted effort by a nation-state to steal its way into a competitive balance with the United States. The longer the United States allows this problem to persist without a proactive plan to counteract China's efforts, the more time we give the Chinese to incorporate our technology into Chinese weapons systems that are not yet, but could one day be, considered on par with United States weaponry.

33 Ioanes, "China Steals US Designs for New Weapons, and It's Getting Away with 'the Greatest Intellectual Property Theft in Human History.'"

34 "Chinese National Who Conspired to Hack into U.S. Defense Contractors' Systems Sentenced to 46 Months in Federal Prison," July 13, 2016, https://www.justice.gov/opa/pr/chinese-national-who-conspired-hack-us-defense-contractors-systems-sentenced-46-months.

35 "Chinese National Who Conspired to Hack into U.S. Defense Contractors' Systems Sentenced to 46 Months in Federal Prison."

36 "Chinese Man to Serve U.S. Prison Term for Military Hacking," *Reuters*, July 14, 2016, https://www.reuters.com/article/us-boeing-cyber-china-idUSKCN0ZT2RQ.

37 "Chinese National Who Conspired to Hack into U.S. Defense Contractors' Systems Sentenced to 46 Months in Federal Prison."

38 "How the US Forced China to Quit Stealing—Using a Chinese Spy," *Wired*, accessed October 19, 2019, https://www.wired.com/story/us-china-cybertheft-su-bin/.

# 3. Anatomy of a Chinese Hacking Organization

China's intelligence capabilities are spread amongst three primary entities. China's Ministry of State Security (MSS) conducts intelligence activities overseas and its Ministry of Public Security is primarily responsible for intelligence activities in China. The People's Liberation Army (PLA) is a Chinese military intelligence organization, but it conducts most of the country's cyber espionage activities.[39] Both the PLA and MSS regularly recruit Chinese citizens travelling to the United States to augment their intelligence activities and enhance placement and access to information.[40] The PLA's cyber command is presumed to be a part of the Third Department, General Staff Department (GSD) of the PLA.[41] The GSD is the equivalent of the United States' Joint Chiefs of Staff and is responsible for formulating doctrine over a wide swath of intelligence and operational capabilities.[42]

In 2013, Mandiant, an American cybersecurity company, identified a Chinese hacking group involved in stealing enormous amounts of data, including the designs for the F-35 Joint Strike Fighter.[43] Mandiant identified the organization as Advanced Persistent Threat 1 (APT 1), which is attributable to Unit 61398 within the PLA.[44] After years of observing APT 1's online activities, Mandiant gained a great deal of insight into the inner workings of the organization and of the identities of those involved in the hacks. In fact, Mandiant became so knowledgeable about Unit 61398's activities that it was able to pierce the military group's anonymity by gaining access to the hackers' laptops, monitoring keystrokes and obtaining photographs of the hackers through the use of their laptops' cameras.[45]

39 Mike Giglio, "China's Spies Are on the Offensive," *The Atlantic*, August 26, 2019, https://www.theatlantic.com/politics/archive/2019/08/inside-us-china-espionage-war/595747/.

40 Giglio.

41 "APT1 Exposing One of China's Cyber Espionage Unit.Pdf," 7, accessed August 24, 2019, https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf.

42 "APT1 Exposing One of China's Cyber Espionage Unit.Pdf," 7.

43 David E. Sanger, *The Perfect Weapon* (Crown Publishing, 2018), 100.

44 Sanger, 101.

45 Sanger, 101–2.

The Mandiant report provided explicit detail of Unit 61398's size, locations, and activities. According to the report, "Unit 61398 [is] located at Datong Road 208 within the Pudong New Area of Shanghai...[a]t 12 stories in height, and offering 130,663 square feet of space, we estimate that this building houses offices for approximately 2,000 people."[46] English-speaking skills and computer acumen were key requirements for assignment into the group: "Unit 61398 appears to be actively soliciting and training English speaking personnel specializing in a wide variety of cyber topics.... Additionally, there is evidence that Unit 61398 aggressively recruits new talent from the Science and Engineering departments of universities such as Harbin Institute of Technology and Zhejiang University School of Computer Science and Technology."[47] The group also enjoyed a significant dedicated support network including a "logistics support unit, outpatient clinic, and kindergarten, as well as guesthouses located both in Gaoqiaozhen and in other locations in Shanghai."[48] The sheer scope and scale of this enterprise signals the significant value the Chinese attached to this effort.

The Mandiant report identified just how prolific APT 1 was. Over the 7 years Mandiant was monitoring APT 1, it discovered that Unit 61398 took hundreds of terabytes of data from more than 140 organizations.[49] The average time APT 1 remained in networks before being discovered was nearly a year - the longest being a period of 4 years and 10 months.[50] In one instance, Mandiant reported Unit 61398 took 10 months to steal nearly 6.5 terabytes of data from one victim alone.[51] Between 2011 to 2013, Mandiant found that Unit 61398 used 832 access points throughout the world to hide their identity and the location from which the breaches were originating.[52]

The Mandiant report received a lot of publicity and focused the United States' attention on the issue in a manner that had never been done

46 "APT1 Exposing One of China's Cyber Espionage Unit.Pdf," 11.

47 "APT1 Exposing One of China's Cyber Espionage Unit.Pdf," 10–11.

48 "APT1 Exposing One of China's Cyber Espionage Unit.Pdf," 16.

49 "APT1 Exposing One of China's Cyber Espionage Unit.Pdf," 20.

50 "APT1 Exposing One of China's Cyber Espionage Unit.Pdf," 21.

51 "APT1 Exposing One of China's Cyber Espionage Unit.Pdf," 25.

52 "APT1 Exposing One of China's Cyber Espionage Unit.Pdf," 40.

before.[53] The report fed into a broader government effort to identify Chinese intrusions, condemn hackers' activity, and attempt to hold them accountable for their actions.[54] To that end, in May 2014, the United States Department of Justice indicted five members of Unit 61398 for conspiring together "to hack into computers of commercial entities...and steal information from those entities that would be useful to their competitors in China, including state-owned enterprises (SOEs)."[55]

## 4. Why is Cyber Espionage Difficult to Stop?

Chinese hacking is facilitated by the somewhat complicated way the Internet functions. To understand how cyber theft happens, it is useful to break down how information is stored and transmitted across the Internet. The Internet is a network of computer networks that communicate with one another using a series of computers, servers, and routers and a set of rules called protocols. These protocols are universally accepted and establish the way messages are sent and received on the Internet. Any device connected to the Internet has a unique designator called an Internet Protocol (IP) address. This address represents the starting or end point for all Internet communications and ensures that a message reaches its desired recipient.

When a user visits a website, the user types the website's name into a browser's address bar and presses the "enter" key. The Internet protocol responsible for sending the request does not operate using words. Rather, it sends the text typed into the address bar to a Domain Name Server which translates the website into an IP address and communicates the information back to the computer. Once the IP address is identified, the user's request is sent to the requested IP address through a series of routers and establishes a connection with the server that holds the content of the

53 John P. Carlin, *Dawn of the Code War* (PublicAffairs, 2018), 245.

54 Carlin, 245.

55 "Indictment, United States v. Wang Dong, et al.," accessed August 24, 2019, https://www.justice.gov/iso/opa/resources/5122014519132358461949.pdf.

web address typed into the address bar. Cyber actors who want to obscure the path taken to launch an attack will take a circuitous path using "hop points" to shroud the IP address where the attack originated, making it harder to accurately attribute the attack.[56]

Internet communication is based on the concept of packet switching. Data is not transmitted in one data burst. Rather, the information is broken into much smaller components called "packets". The packets are sent to the IP address that requested the information via hardware called routers. The router identifies the most efficient path for the packets to travel and sends them in that direction. The packets are reassembled by an Internet protocol on the recipient's computer and the computer displays the information sent or requested.

A packet is comprised of three components: the header, the trailer and the payload. Each component plays a key role in how packets are routed and reassembled. Essentially, the header contains the sender's IP address, the receiver's IP address, and the packet number - which helps the system sequence the reassembly of the packets upon receipt. The payload contains the chunk of data that is being sent or requested. The trailer contains some information to inform the system that there is no more data in the packet. Since information is disassembled into packets before it is sent on the Internet, it is not possible to simply look at the network traffic to ascertain what a cyber actor is stealing from a network. Network security personnel are required to use protocol analyzers, like commercially-available Wireshark, to examine the packets' payload to make sense of what is entering or leaving the network.[57] Since the adversary knows that network owners have this capability, it will often resort to encrypting its traffic utilizing a Virtual Private Network (VPN) and tunneling into a network to prevent their activities from being discovered.[58]

56 Ms. Smith, "US Charges 3 Chinese Security Firm Hackers with Cyber Espionage," CSO Online, November 28, 2017, https://www.csoonline.com/article/3238828/us-charges-3-chinese-security-firm-hackers-with-corporate-cyber-espionage.html.

57 "Wireshark · Go Deep.," accessed November 1, 2019, https://www.wireshark.org/.

58 "Chinese Hackers Using 'Terracotta' VPN to Hijack Servers of Small Businesses and Attack Government Sites | South China Morning Post," accessed November 1, 2019, https://www.scmp.com/tech/enterprises/article/1846706/chinese-hackers-using-vpn-hijack-servers-unsecure-small-businesses.

Encryption is a form of cryptography that arranges the contents of data so that it is indecipherable to someone who does not have a proper key to unlock the encryption.[59] Encryption levels are measured by the length of the key used to decipher the encrypted data. So, a 128-bit key is shorter and less complicated than a 256-bit key. Nonetheless, the sheer number of possible combinations makes encryption using either key impossible to break using current-day technology; a 256-bit key can create over 115 quattuorvigintillion (a 78-digit number) variations.[60] Thus, even with a protocol analyzer, network security personnel are not able to identify what is entering or leaving its network if the data is encrypted.

Most of the infrastructure for a company's network operations relies upon software to run its hardware and allow everything to function properly. Hardware and software engineers sometimes create "backdoors" in their products to allow access into a system when users are otherwise blocked from doing so. Backdoors can also be manufactured by hackers who identify vulnerabilities in coding of the software or the security configurations for the hardware.[61] Once the unauthorized user gains access to the system, they can mine the network for credentials of authorized users and use them to gain access to the network's most valuable data without alerting network security mechanisms to their presence.[62]

Companies can protect their systems against unauthorized entry by closely monitoring activity on their networks and updating the cybersecurity software running on their system. Intrusion detection systems (IDSs) can be designed to identify irregular network traffic or the "signature" of known adversarial actors and prevent them from entering the system.[63] A signature is a characteristic of the network traffic that cybersecurity experts or law enforcement representatives have identified as being associated with

59 "What Is Data Encryption?," Forcepoint, December 4, 2018, https://www.forcepoint.com/cyber-edu/data-encryption.

60 "Learn Cryptography - Why Is 2^256 Secure?," accessed October 4, 2019, https://learncryptography.com/cryptanalysis/why-is-2-256-secure.

61 Catalin Cimpanu, "Researchers Find Stealthy MSSQL Server Backdoor Developed by Chinese Cyberspies," ZDNet, accessed November 1, 2019, https://www.zdnet.com/article/researchers-find-stealthy-mssql-server-backdoor-developed-by-chinese-cyberspies/.

62 "Compromised Credentials: The Primary Point of Attack for Data Breaches | securityweek.com," accessed November 1, 2019, https://www.securityweek.com/compromised-credentials-primary-point-attack-data-breaches.

63 "Intrusion Detection System (IDS)," *GeeksforGeeks* (blog), April 8, 2019, https://www.geeksforgeeks.org/intrusion-detection-system-ids/.

a threat actor. For instance, a company's IDS would create an alert for any traffic trying to enter the network from an IP address that matches an IP address linked to a past intrusion. A signature-based IDS also activates on known malware exploits; therefore, if a threat actor launches an attack using a different set of signatures or it changes a small characteristic of the known exploit, the signature-based model will fail to identify the threat and the attack will be allowed to proceed. Furthermore, VPNs can shroud the identity of the known IP address of a malicious actor and are capable of allowing an intruder to avoid detection by an IDS.[64]

The most prevalent manner of hacking involves finding an unwitting accomplice on the inside of a system and exploit their carelessness. Hackers commonly try to gain access to a computer network through a spear phishing email. In a spear phish effort, the threat actor poses as someone who the user trusts or knows and sends an email in which the user is asked to click on an embedded link or attachment.[65] The link or attachment typically contains a line of code or malicious software that creates an opening into the system that the hacker can use to gain entry into the network.[66] Once in the network, the hacker will review the contents of the network and exfiltrate data that is believed to be of value. To obscure the data exfiltration from discovery, hackers will break data into smaller files and hide the data flow within legitimate traffic transiting the network. In Su Bin's cyber espionage case referenced herein, Su sent his co-conspirators the names of people working within the aerospace industry.[67] In turn, the co-conspirators sent phishing emails to the names on the list to gain entry into the networks and steal the data.[68] The emails were crafted to appear as if they were sent by someone the targets knew and contained an

64 "A VPN Masks Your Real IP Address. How It Does That Will Amaze You.," WhatIsMyIPAddress.com, accessed November 1, 2019, https://whatismyipaddress.com/vpn-service.

65 "What Is Spear-Phishing? Defining and Differentiating Spear-Phishing from Phishing," Text, Digital Guardian, June 27, 2016, https://digitalguardian.com/blog/what-is-spear-phishing-defining-and-differentiating-spear-phishing-and-phishing.

66 Zak Doffman, "Chinese State Hackers Suspected of Malicious Cyber Attack on U.S. Utilities," Forbes, accessed November 1, 2019, https://www.forbes.com/sites/zakdoffman/2019/08/03/chinese-state-hackers-suspected-of-malicious-cyber-attack-on-u-s-utilities/.

67 "How the US Forced China to Quit Stealing—Using a Chinese Spy."

68 "How the US Forced China to Quit Stealing—Using a Chinese Spy."

attachment that, if clicked, surreptitiously connected the target's computer with a computer controlled by the Chinese hackers.[69]

Ultimately, the only way to truly protect a network from being hacked through the Internet is to completely isolate it from the Internet. This can be done without eliminating the highly desirable collaborative benefits of the connected networks. By implementing a controlled number of highly secured and heavily monitored gateways, a company can reduce the number of nodes to protect. While this approach would need to be optimized to limit lag time,[70] a sub-second response time is not generally required in a research and development setting. Although this approach would harden the system against an Internet intrusion, the isolated system would still be vulnerable to an insider who is able to directly access the computer network and originate an exploit from within the infrastructure.

# 5. Proposed Solutions

The previous discussion reveals the scope of the Chinese cyber espionage threat and the way the Chinese are using the Internet to steal the United States' secrets. The problem is multi-faceted and complex, so there is no single solution. Wholly detaching the company or research institute from the Internet would solve the problem; however, from a practical perspective it is not considered as part of these proposed solutions. Instead, it is much more useful to think of the following solutions in terms of a suite of options to be implemented in a layered approach by policy makers and cybersecurity experts that can collectively help thwart the Chinese from stealing this valuable data. These suggestions leverage resources and capabilities of the United States government and the organizations that are the target of these intrusions. These proposals spread the responsibility of

69 Jim Sciutto, "The Chinese Businessman Who Conned U.S. Defense Contractors," *The Daily Beast*, May 19, 2019, sec. arts-and-culture, https://www.thedailybeast.com/the-friendly-chinese-businessman-who-made-fools-of-us-defense-contractors.

70 "2020 Network Latency Guide: How to Check, Test, & Reduce," DNSstuff, August 19, 2019, https://www.dnsstuff.com/network-latency. The time it takes for information to be sent and received is referred to "network latency". The calculation is measured in terms of milliseconds. Thus, assuming the network activity does not require virtually instantaneous response times, users will likely not notice the time delay caused by the monitoring activity.

addressing this threat amongst key stakeholders and represents a philosophy that no single solution can possibly be effective.

## Proposal #1: Authorize DOD to Secure Private Networks

In Homeland Security Presidential Directive (HSPD) 7, the President designated the Department of Defense as the Sector-Specific Agency (SSA) responsible for the Defense Industrial Base (DIB).[71] HSPD 7 vests SSAs with the authority to "collaborate with all Federal departments and agencies, State and local governments and the private sector...in their infrastructure sector," "conduct or facilitate vulnerability assessments of the sector," and "encourage risk management strategies to protect and mitigate the effects of attacks."[72] The program, however, does not permit the DOD to provide protection for private networks without first obtaining authorization to do so from the President.[73] This structure is a good first step, but it needs to be expanded to provide DOD with the ability to provide network security to DIB organizations that request the assistance.

When assessing this proposal, it is useful to consider it within the context of the three components of a traditional cybersecurity strategy. The first involves a perimeter or gateway defense. The tools for this component are emplaced on the outside of a network and help identify and prevent known adversaries and malware from entering and compromising a network. The second component involves the use of software to constantly monitor activity inside the network to identify and thwart anomalous actions taken by adversaries who may have avoided detection by the perimeter defense. The third component involves the development of a comprehensive training program to help users identify common tactics employed by intruders that trick a user into granting that intruder with trusted network permissions, thus allowing the intruder to have unfettered access to sensitive

71 "Homeland Security Presidential Directive 7," Department of Homeland Security, June 27, 2008, https://www.dhs.gov/homeland-security-presidential-directive-7.

72 "Homeland Security Presidential Directive 7."

73 "Defense Industrial Base Sector-Specific Plan 2010.Pdf," 6, accessed November 1, 2019, https://www.dhs.gov/sites/default/files/publications/nipp-ssp-defense-industrial-base-2010-508.pdf.

data within the system. This proposal fits within the perimeter or gateway defense component of an entity's cybersecurity strategy.

As described herein, the current cybersecurity posture for the nation is woefully inadequate and the evidence is overwhelming that private industry is either incapable of, or not interested in, confronting the cyber espionage threat on its own. In instances where there is a clear DOD equity in the information at stake, DOD must be granted the authority to provide network security for companies and institutions that retain DOD-related information. This would be entirely based on the consent of the network owner and strict notification guidelines to inform network users of DOD's presence within the system. This proposal, however, is bound to generate controversy. Undeniably, the DOD's mission is to fight and win the nation's wars - not protect private computer networks. When sensitive DOD-related information resides on a computer network, however, there is a significant enough nexus between the DOD protecting the information and preserving DOD's ability to fight and win those wars.

The United States Constitution and the federal statutes governing electronic surveillance limit the authority of the federal government to engage in activities that allow it to monitor and react to instances of cyber espionage occurring in private computer networks within the United States. From a constitutional perspective, the Fourth Amendment protects people against unreasonable searches and seizures without consent or a judicial warrant. Likewise, the Wiretap Act,[74] the Stored Communications Act (SCA),[75] and the Pen Register/Trap and Trace statute[76] prevent the government from conducting electronic surveillance activities without judicial approval and authorization. Both the constitutional and statutory prohibitions, however, are designed to confront situations wherein the government is conducting the activity without the consent of the network owner or the person being monitored. To the extent the government

74 "18 U.S. Code § 2511 - Interception and Disclosure of Wire, Oral, or Electronic Communications Prohibited," LII / Legal Information Institute, accessed January 25, 2020, https://www.law.cornell.edu/uscode/text/18/2511.

75 "18 U.S. Code Chapter 121 - Stored Wire and Electronic Communications and Transactional Records Access," LII / Legal Information Institute, accessed January 25, 2020, https://www.law.cornell.edu/uscode/text/18/part-I/chapter-121.

76 "18 U.S. Code Chapter 206 - Pen Registers and Trap and Trace Devices," LII / Legal Information Institute, accessed January 25, 2020, https://www.law.cornell.edu/uscode/text/18/part-II/chapter-206.

obtains informed consent from the network users, the constitutional and statutory concerns appear to be assuaged.[77]

Under the current Defense Industrial Base (DIB) program, the DOD can enter into threat-based information sharing agreements with members of the DIB that allows for mutual cooperation in identifying threat signatures and exploit patterns of the adversary.[78] Information sharing is a useful tool to help prevent adversaries from gaining unauthorized access into the network by notifying network owners of potential threats of which they may not have been aware, but these information sharing arrangements provide no protection to the information once an adversary breaches a network. Likewise, information sharing is not useful in determining what information the adversary is accessing, what methods the adversary is using to operate within the system and what information the adversary is exfiltrating. These are all critical questions to answer when trying to determine the identity of the intruder, the nature of the information that intruder stole, and the methods the intruder used to identify and exfiltrate the information. DOD has the capability to gather that information, but it currently lacks the jurisdiction to employ those capabilities.

Despite DOD's cyber capabilities, the private sector may not be inclined to accept DOD cybersecurity support - even if it could be offered. In July 2017, the Naval War College conducted a wargame with almost 125 local, state, federal and private sector partners to analyze the effects of a cyber breach and the level at which a DOD response would be justified.[79] The two-day event included more than 60 notional cyber intrusions covering 14 critical infrastructure sectors.[80] After observing the exercise and reviewing feedback from the participants, a Naval War College professor observed that the private sector seemed to conclude that DOD should

77 "Legal Issues Relating to the Testing, Use and Deployment of an Intrusion-Detection System (Einstein 2.0) to Protect Unclassified Computer Networks in the Executive Branch," accessed August 19, 2019, https://www.justice.gov/sites/default/files/olc/opinions/2009/01/31/e2-issues_0.pdf.

78 "DIB Fact Sheet.Pdf," accessed October 3, 2019, https://dodcio.defense.gov/Portals/0/Documents/DIB%20Fact%20Sheet.pdf.

79 "Cyber Attacks on Critical Infrastructure: Insights from War Gaming," War on the Rocks, July 26, 2017, https://warontherocks.com/2017/07/cyber-attacks-on-critical-infrastructure-insights-from-war-gaming/.

80 "Cyber Attacks on Critical Infrastructure."

focus on stopping cyber intrusions from occurring in the first place rather than enhancing cybersecurity efforts of the private sector.[81]

As described herein, successfully preventing nation-states from conducting cyber intrusions is an almost impossible task. The more effective way of confronting this threat is via a robust cyber defense posture at the point of attack. The private sector is not capable of preventing China from utilizing its vast well of resources and personnel to steal information residing in private networks. This is not surprising considering the concerted efforts China is taking to steal the information. Consequently, in order to even the playing field, DOD must be permitted to contribute its expertise and resources to provide cybersecurity protection to DIB organizations that ask for the assistance. If the DOD, as the SSA of the DIB, is ultimately responsible for protecting the integrity of the DIB's networks, preventing it from providing cybersecurity protection seems to limit the likelihood of achieving tangible success in this area.

## Proposal #2: Allow Companies to "Hack Back"

If DOD is not going to be authorized to operate on the periphery of private networks to offer cybersecurity protection, the country must consider giving the private sector some limited authority to reach into the Internet and take back that which has been stolen from them. Typically referred to as "hack back," this proposal refers to the ability of a company whose information is being stolen to respond by stopping the theft from occurring and deleting the information from the thieves' network, thus preventing the adversary from benefitting from the theft. This is a form of self-help that acknowledges that government agencies are oftentimes reluctant to effectively respond to an intrusion or are incapable of dedicating resources or expertise to the problem.

This may seem like a radical proposal; however, the concept is not much different from how governments dealt with the confounding problem of

81 "Cyber Attacks on Critical Infrastructure."

pirates on the high seas for centuries. Starting as early as the 13th century, countries began authorizing privateers to act as an arm of the state to confront their enemies during a state of conflict.[82] Likewise, up until the 19th century, states in peacetime environments issued *letters of marque* to victims of pirate attacks authorizing the holder of the *letter of marque* to pursue retribution for the theft by attacking ships belonging to the aggressor nation in order to procure property that would compensate for the victims' losses.[83] Currently, the Computer Fraud and Abuse Act (CFAA) prevents companies from hacking back; however, Congress has been considering legislation that would permit companies to hack back to "establish attribution", "disrupt unauthorized activity" and "monitor the behavior to assist in developing future intrusion prevention".[84]

Hacking back carries with it a certain degree of risk that makes this an extremely controversial option. There is always the risk of a private entity misattributing the perpetrator or damaging a network that was not involved in the theft. Further, the response, even if properly attributed, may result in an escalation of activities against the network owner or others associated with the network. Moreover, the hack back activity may limit or affect potential response options and activities available to law enforcement and intelligence organizations that dedicate resources and personnel to respond to the threat. These concerns can be mitigated or eliminated entirely if the entity hacking back is required to do so under the supervision and control of the DOD. Moreover, in order to engage in hack back activities the government could issue a license to companies capable of demonstrating they have a minimum level of expertise in responsibly executing the hack back and requiring that all hack back activities are coordinated with and through the DOD and the Intelligence Community. Furthermore, the government will have to closely regulate and control the hack back options available to these licensees and prevent the private entities from maliciously damaging an adversary's networks or detrimentally impacting information residing on those networks. The CFAA will likely have to be amended since the hack back actors may have to cause

82 "Egloff - Cybersecurity and the Age of Privateering A Historical Analogy.Pdf," 3–4, accessed October 17, 2019, https://www.politics.ox.ac.uk/materials/publications/14938/workingpaperno1egloff.pdf.

83 "Egloff - Cybersecurity and the Age of Privateering A Historical Analogy.Pdf," 4.

84 "Hackback Is Back: Assessing the Active Cyber Defense Certainty Act," Lawfare, June 14, 2019, https://www.lawfareblog.com/hackback-back-assessing-active-cyber-defense-certainty-act.

temporary adverse effects on the hostile actor's networks to gain remote access to the system and either retrieve or erase the stolen data.

## Proposal #3: Create Financial Incentives for Private Cybersecurity

Few things motivate private industry more than financial incentives and penalties. The government must incentivize contractors and research institutes by giving preferential treatment in bid proposals to those entities that establish robust cybersecurity measures. This may result in higher upfront costs for government contracts but more secure networks will help reduce the crippling financial and competitive costs associated with cyber intrusions and theft.

Additionally, the government must sue companies for punitive or compensatory damages for losses when those companies fail to take reasonable steps to protect their networks against a breach. At a minimum, why should the company or institute keep the money the government paid for the research when that company or institute fails to take appropriate measures to protect the government's investment? Under this proposal, a liability determination would hinge on whether the company took necessary and appropriate steps to prevent the intrusion and whether the breach was foreseeable based on all available information. This proposal would be reinforced with language inserted into all government defense contracts that requires a government contractor to utilize industry-accepted cybersecurity protections, such as those proposed by the National Institute for Standards and Technology (NIST).[85]

There are a significant number of actions an organization can take to place itself in a stronger cybersecurity posture that would make it harder for an adversary to gain unauthorized access to its networks. First, make cybersecurity a priority. It must be a topic of discussion for employees the moment they are hired and throughout their time with the organization.

85 National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1" (Gaithersburg, MD: National Institute of Standards and Technology, April 16, 2018), https://doi.org/10.6028/NIST.CSWP.04162018.

The discussion can be generated by regular training sessions for employees on simple cybersecurity practices. Sensitizing employees to the potential danger of responding to spear phish emails or inserting digital media given to them by a third party into the company's digital systems can go a long way in preventing unauthorized access into digital systems.

Companies must also have cybersecurity software that identifies anomalous activity on its network. This should be an unconditional requirement for any company doing business with the United States government. However, it is not enough to simply have the security software running on the network - the software, as well as all the other elements of the network, must be regularly patched with updates that reflect repairs to newly discovered vulnerabilities in the system. As a cost of doing business with the United States, these companies must incorporate mandated and auditable security requirements. If they refuse, they are removed from the approved DOD contractors' list and prohibited from bidding on DOD contracts.

Consider the 2017 Equifax breach in gaining a better understanding of the worthlessness of a network that is not adequately patched. In the Equifax case, the Chinese exploited a vulnerability in a publicly identified weakness in the software running an operating system on Equifax's network to help steal the financial credit histories of nearly 150 million people in the United States.[86] The Chinese began the cyber attack more than 60 days after the notification of the vulnerability was released to the world - plenty of time for Equifax to patch the vulnerability and prevent the massive data theft from occurring.[87] Equifax, however, never employed the patch because a senior official failed to forward an email to technicians that would have informed the technicians that a vulnerability patch was necessary.[88]

In order to avoid this issue altogether, the government needs to stop conducting business with companies or research institutes that are incapable of providing an adequate level of cybersecurity. This may result in sidelining smaller companies from a competitive bidding process, but it is the most

86 "Equifax-Report.Pdf," 27, accessed October 14, 2019, https://republicans-oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf.

87 "Equifax-Report.Pdf," 31.

88 "U.S. House of Representatives Committee on Oversight and Government Reform Report on the Equifax Data Breach," 50, accessed January 7, 2020, https://republicans-oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf.

rational way to help confront this threat. The cybersecurity posture of a proposing entity must be considered in conjunction with the remainder of its bid and should be compared against the capabilities of others in competition for the awarded contract. Under this paradigm, it would be possible for a contract to be awarded to a more expensive bid if that company presented a more robust cybersecurity infrastructure than others in competition for the award. As the nature of the contract involves increasingly more sensitive matters, the weight the government attaches to the cybersecurity capabilities of the awardee increases in relation to the other aspects of the competitor's proposals. This approach to government contracting will send the message to competitors that cybersecurity must be prioritized when competing for lucrative government contracts in the future.

## Proposal #4: Increased Emphasis on Prosecution

Prosecuting offenders will hold individual actors accountable for their actions and, in theory, deter China from conducting similar activities in the future. Indicting and prosecuting individuals in these cases can be a challenge. Many times, the sources and methods used for collecting the information are sensitive and too valuable to reveal. Despite this challenge, there are several ways to attribute an attack that may not require the government to reveal the methods it employed to detect the breach.[89] The Department of Justice has been able to lodge indictments against individuals involved in state-sponsored cyber espionage, so it can and has been done in a manner that does not jeopardize intelligence secrets.[90][91]

Given the startling nature of the scope and scale of the Chinese cyber espionage efforts, some have criticized prosecutions as being an ineffective

89 "ODNI_A_Guide_to_Cyber_Attribution.Pdf," accessed September 22, 2019, https://www.dni.gov/files/CTIIC/documents/ODNI_A_Guide_to_Cyber_Attribution.pdf.

90 "Chinese Professors Among Six Defendants Charged with Economic Espionage and Theft of Trade Secrets for Benefit of People's Republic of China — FBI," Press Release, accessed September 22, 2019, https://www.fbi.gov/contact-us/field-offices/sanfrancisco/news/press-releases/chinese-professors-among-six-defendants-charged-with-economic-espionage-and-theft-of-trade-secrets-for-benefit-of-peoples-republic-of-china.

91 "Chinese Hackers Indicted," Story, Federal Bureau of Investigation, accessed September 22, 2019, https://www.fbi.gov/news/stories/chinese-hackers-indicted-122018.

strategy to confront Chinese cyber espionage efforts.[92] Detractors argue that the relatively minor cost imposed by the "naming and shaming" of a prosecution does not compare against the significant value China derives from its illicit activities.[93]

This criticism can be addressed simply by initiating *more* prosecutions. Aside from reducing the number of active cyber espionage events, there are several indirect benefits to prosecution. First, additional prosecutions will serve to inform the public of the scope and scale of the problem the United States is confronting.[94] Second, news coverage and press briefings on these prosecutions can serve as a useful tool in generating dialogue within the cybersecurity community and a catalyst to emphasizing the importance of cybersecurity of computer networks.[95] Third, indictments prevent named defendants from travelling to areas where the United States enjoys extradition agreements.[96] Fourth, successful prosecutions can serve as a mechanism to levy stiff economic sanctions against a Chinese company operating in the United States that utilizes stolen information in the development and production phases of its business.[97] The foregoing benefits of prosecution should incentivize prosecutors to indict more Chinese government officials who are involved in all planning and approval stages of the attack.

## Proposal #5: Data Obfuscation

As described herein, China is motivated to seek out and steal the results of technological research and development belonging to the United States and the Defense Industrial Base (DIB). If we accept that China will find a way to pierce the security of our networks, the United States and members of

92 "Charges Against Chinese Hackers Are Now Common. Why Don't They Deter Cyberattacks?," NPR.org, accessed October 19, 2019, https://www.npr.org/2019/02/05/691403968/charges-against-chinese-hackers-are-now-common-why-dont-they-deter-cyberattacks.

93 "Charges Against Chinese Hackers Are Now Common. Why Don't They Deter Cyberattacks?"

94 "Threat Analyst Insights: The Impact of Indicting Foreign Nationals in Cyberespionage Cases," *Recorded Future* (blog), September 27, 2018, https://www.recordedfuture.com/foreign-cyberespionage-cases/.

95 "Threat Analyst Insights."

96 "Threat Analyst Insights."

97 "A New Old Threat: Countering the Return of Chinese Industrial Cyber Espionage," accessed September 2, 2019, https://www.cfr.org/report/threat-chinese-espionage.

the DIB will have to employ measures making it more difficult for intruders to identify and access information when they breach the system. Data obfuscation methods such as data masking[98] and zero-trust architecture[99] can help prevent intruders from accessing crucial files or understanding the contents of those files once accessed.

The concept underlying data masking is simple. If you accept that it is nearly impossible to prevent intrusions from occurring, why not make it difficult for the adversary to find what they are looking for when they enter the system? Encrypting data residing on a network (a form of data masking) is one way to prevent the adversary from gaining access to information once it is inside a network; however, sloppy cybersecurity practices can quickly eliminate the benefit of this cybersecurity measure.

For instance, in 2018, the Chinese hacked into Marriott's reservation system and stole personal data (including passport numbers and credit card information) belonging to 500 million Marriott customers. Marriott encrypted the credit card data on its network, but the hackers were able to take the encryption keys for the encryption algorithm - thus, rendering the encryption effort useless.[100] Other data masking techniques include character scrambling (wherein the data is jumbled in such a manner that the information is unintelligible); "nulling out" (data is null for anyone not authorized to access the information); and substitution (realistically invalid data is substituted for actual data).[101]

Zero-trust architecture is based on the concept that the network should not trust anyone trying to access data residing in the system.[102] In order to gain access to files, a user is required to present credentials to unlock information they are trying to access. This will help prevent an adversary from

98 "What Is Data Masking? Data Masking Explained—BMC Blogs," accessed October 2, 2019, https://www.bmc.com/blogs/data-masking/.

99 "What Is a Zero Trust Architecture? - Palo Alto Networks," accessed October 2, 2019, https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture.

100 Taylor Telford, "Marriott Discloses Massive Data Breach Affecting up to 500 Million Guests," Washington Post, accessed October 14, 2019, https://www.washingtonpost.com/business/2018/11/30/marriott-discloses-massive-data-breach-impacting-million-guests/.

101 "What Is Data Masking? Data Masking Explained—BMC Blogs," accessed October 14, 2019, https://www.bmc.com/blogs/data-masking/.

102 "What Is a Zero Trust Architecture? - Palo Alto Networks," accessed October 14, 2019, https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture.

gaining access to a network and having open access to everything stored there. In a zero-trust architecture environment, the adversary will have to obtain the credentials of someone who has authorization to access the information to read its contents. One can imagine the utility of this technique when used in conjunction with the data masking system described above.

Obviously, none of these techniques will be effective if the adversary is able to gain access to the credentials of authorized users on the network or the encryption keys for the encrypted data. This concern can be ameliorated by storing credentials and keys in a manner that will only permit a limited number of trusted individuals to access the information. The credentials and keys must also be cordoned-off from the rest of the network so that if an intruder is able to access the system, it will be sealed-off from the mechanisms that will allow them to access the protected information.

# 6. Conclusion

By 2025, cybersecurity costs across the globe are reported to approach $1 trillion dollars.[103] However, protecting computer networks with expensive cyber defenses is only part of the solution. The most expensive cybersecurity system will fail if organizations or its users do not practice good cybersecurity practices. Human-caused mistakes are responsible for 90 percent of all data breaches.[104] A survey of six million users within 11,000 differently-sized organizations determined that approximately 27 percent of users opened a phishing email or link upon receipt.[105] This concept of human error or vulnerability is unavoidable and makes the threat of Chinese hacking into DIB organizations an inevitable threat.[106] Consequently, the approach to address this problem must be comprehensive and wide-ranging.

Chinese cyber espionage efforts are allowing that nation to steal the DOD's intellectual property at an astounding rate. As a result, the United States is facing the very real prospect of fighting a future conflict against an adversary equipped with hardware and software that is largely derived from technology researched and developed by United States companies. In order to confront this problem, the United States should permit the DOD to monitor and defend private networks affiliated with the DOD research and development. Furthermore, Congress must pass legislation that would authorize companies, in coordination with the DOD, to respond to a cyber intrusion by stopping the attack and deleting its stolen information. Additionally, incentivizing companies doing business with the DOD and holding the victimized company financially liable for not adequately protecting its network against foreseeable cyber risks, prosecuting those responsible for cyber espionage, and encouraging companies to harden their information security standards are three additional ways the United States can confront this confounding threat to national security.

103 "Global Cybersecurity Spending Predicted to Exceed $1 Trillion From 2017-2021," *Cybercrime Magazine* (blog), June 10, 2019, https://cybersecurityventures.com/cybersecurity-market-report/.

104 Anthony Spadafora, "90 Percent of Data Breaches Are Caused by Human Error," TechRadar, accessed November 3, 2019, https://www.techradar.com/news/90-percent-of-data-breaches-are-caused-by-human-error.

105 DH Kass, "Study: Phishing Scams Dupe More Than 30 Percent of Insurance, Non-Profit Employees," MSSP Alert, January 26, 2018, https://www.msspalert.com/cybersecurity-news/study-phishing-scams-dupe-more-than-30-percent-of-insurance-non-profit-employees/.

106 Kass.

# Bibliography

"2017_PRC_NationalIntelligenceLaw.Pdf." Accessed October 5, 2019. http://cs.brown.edu/courses/csci1800/sources/2017_PRC_NationalIntelligenceLaw.pdf.

"A New Old Threat: Countering the Return of Chinese Industrial Cyber Espionage." Accessed September 2, 2019. https://www.cfr.org/report/threat-chinese-espionage.

"A New Old Threat: Countering the Return of Chinese Industrial Cyber Espionage." Accessed September 2, 2019. https://www.cfr.org/report/threat-chinese-espionage.

"After a Hiatus, China Accelerates Cyberspying Efforts to Obtain U.S. Technology - The New York Times." Accessed September 1, 2019. https://www.nytimes.com/2018/11/29/us/politics/china-trump-cyberespionage.html.

"APT1 Exposing One of China's Cyber Espionage Unit.Pdf." Accessed August 24, 2019. https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf.

Carlin, John P. *Dawn of the Code War*. PublicAffairs, 2018.

"China Knows All About the F-35 and F-22 (Thanks to the Data It Stole) | The National Interest." Accessed September 4, 2019. https://nationalinterest.org/blog/buzz/china-knows-all-about-f-35-and-f-22-thanks-data-it-stole-61912.

"Chinese Hackers Indicted." Story. Accessed September 22, 2019. https://www.fbi.gov/news/stories/chinese-hackers-indicted-122018.

"Chinese Hackers Using 'Terracotta' VPN to Hijack Servers of Small Businesses and Attack Government Sites | South China Morning Post." Accessed November 1, 2019. https://www.scmp.com/tech/enterprises/article/1846706/chinese-hackers-using-vpn-hijack-servers-unsecure-small-businesses.

"Chinese Man to Serve U.S. Prison Term for Military Hacking." *Reuters*, July 14, 2016. https://www.reuters.com/article/us-boeing-cyber-china-idUSKCN0ZT2RQ.

"Chinese National Who Conspired to Hack into U.S. Defense Contractors' Systems Sentenced to 46 Months in Federal Prison," July 13, 2016. https://www.justice.gov/opa/pr/chinese-national-who-conspired-hack-us-defense-contractors-systems-sentenced-46-months.

"Chinese Professors Among Six Defendants Charged with Economic Espionage and Theft of Trade Secrets for Benefit of People's Republic of China — FBI." Press Release. Accessed September 22, 2019. https://www.fbi.gov/contact-us/field-offices/sanfrancisco/news/press-releases/chinese-professors-among-six-defendants-charged-with-economic-espionage-and-theft-of-trade-secrets-for-benefit-of-peoples-republic-of-china.

Cimpanu, Catalin. "Researchers Find Stealthy MSSQL Server Backdoor Developed by Chinese Cyberspies." ZDNet. Accessed November 1, 2019. https://www.zdnet.com/article/researchers-find-stealthy-mssql-server-backdoor-developed-by-chinese-cyberspies/.

"Compromised Credentials: The Primary Point of Attack for Data Breaches | Securityweek.Com." Accessed November 1, 2019. https://www.securityweek.com/compromised-credentials-primary-point-attack-data-breaches.

Cooper, Zack. "Understanding the Chinese Communist Party's Approach to Cyber-Enabled Economic Warfare," September 2018, 44.

CPO Magazine. "New CNCERT Report Shows Most Cyber Attacks on China Originate from United States," June 24, 2019. https://www.cpomagazine.com/cyber-security/new-cncert-report-shows-most-cyber-attacks-on-china-originate-from-united-states/.

Cybercrime Magazine. "Global Cybersecurity Spending Predicted To Exceed $1 Trillion From 2017-2021," June 10, 2019. https://cybersecurityventures.com/cybersecurity-market-report/.

Department of Homeland Security. "Defense Industrial Base Sector," June 12, 2014. https://www.dhs.gov/cisa/defense-industrial-base-sector.

Department of Homeland Security. "Homeland Security Presidential Directive 7," June 27, 2008. https://www.dhs.gov/homeland-security-presidential-directive-7.

"Defense Industrial Base Sector-Specific Plan 2010.Pdf." Accessed November 1, 2019. https://www.dhs.gov/sites/default/files/publications/nipp-ssp-defense-industrial-base-2010-508.pdf.

"DIB Fact Sheet.Pdf." Accessed October 3, 2019. https://dodcio.defense.gov/Portals/0/Documents/DIB%20Fact%20Sheet.pdf.

Digital Guardian. "What Is Spear-Phishing? Defining and Differentiating Spear-Phishing from Phishing." Text, June 27, 2016. https://digitalguardian.com/blog/what-is-spear-phishing-defining-and-differentiating-spear-phishing-and-phishing.

DNSstuff. "2020 Network Latency Guide: How to Check, Test, & Reduce," August 19, 2019. https://www.dnsstuff.com/network-latency.Federal Bureau of Investigation.

"DOD Releases Fiscal Year 2020 Budget Proposal, U.S. Department of Defense Release". Accessed September 2, 2019. https://www.defense.gov/Newsroom/Releases/Release/Article/1782623/dod-releases-fiscal-year-2020-budget-proposal/.

Doffman, Zak. "Chinese State Hackers Suspected Of Malicious Cyber Attack On U.S. Utilities." Forbes. Accessed November 1, 2019. https://www.forbes.com/sites/zakdoffman/2019/08/03/chinese-state-hackers-suspected-of-malicious-cyber-attack-on-u-s-utilities/.

"Egloff - Cybersecurity and the Age of Privateering a History.Pdf." Accessed October 17, 2019. https://www.politics.ox.ac.uk/materials/publications/14938/workingpaperno1egloff.pdf.

"Equifax-Report.Pdf." Accessed October 14, 2019. https://republicans-oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf.

Forcepoint. "What Is Data Encryption?," December 4, 2018. https://www.forcepoint.com/cyber-edu/data-encryption.

GeeksforGeeks. "Intrusion Detection System (IDS)," April 8, 2019. https://www.geeksforgeeks.org/intrusion-detection-system-ids/.

Giglio, Mike. "China's Spies Are on the Offensive." *The Atlantic*, August 26, 2019. https://www.theatlantic.com/politics/archive/2019/08/inside-us-china-espionage-war/595747/.

Hollings, Alex. "Counterfeit Air Power: Meet China's Copycat Air Force." Popular Mechanics, September 19, 2018. https://www.popularmechanics.com/military/aviation/g23303922/china-copycat-air-force/.

"How the US Forced China to Quit Stealing—Using a Chinese Spy." *Wired*. Accessed October 19, 2019. https://www.wired.com/story/us-china-cybertheft-su-bin/.

"Indictment, United States v. Wang Dong, et Al." Accessed August 24, 2019. https://www.justice.gov/iso/opa/resources/5122014519132358461949.pdf.

Ioanes, Ellen. "China Steals US Designs for New Weapons, and It's Getting Away with 'the Greatest Intellectual Property Theft in Human History.'" Business Insider. Accessed October 19, 2019. https://www.businessinsider.com/esper-warning-china-intellectual-property-theft-greatest-in-history-2019-9.

"IP_Commission_Report_Update_2017.Pdf." Accessed August 24, 2019. http://www.ipcommission.org/report/IP_Commission_Report_Update_2017.pdf.

"John C. Demers, Assistant Attorney General, National Security Division, Department of Justice, Statement before the Senate Committee on the Judiciary, 'China's Non-Traditional Espionage Against the United States, The Threat and Potential Policy Responses,'" December 12, 2018, 10.

Kass, DH. "Study: Phishing Scams Dupe More Than 30 Percent of Insurance, Non-Profit Employees." MSSP Alert, January 26, 2018. https://www.msspalert.com/cybersecurity-news/study-phishing-scams-dupe-more-than-30-percent-of-insurance-non-profit-employees/.

Lawfare. "Hackback Is Back: Assessing the Active Cyber Defense Certainty Act," June 14, 2019. https://www.lawfareblog.com/hackback-back-assessing-active-cyber-defense-certainty-act.

"Learn Cryptography - Why Is 2^256 Secure?" Accessed October 4, 2019. https://learncryptography.com/cryptanalysis/why-is-2-256-secure.

"Legal Issues Relating to the Testing, Use and Deployment of an Intrusion-Detection System (Einstein 2.0) to Protect Unclassified Computer Networks in the Executive Branch." Accessed August 19, 2019. https://www.justice.gov/sites/default/files/olc/opinions/2009/01/31/e2-issues_0.pdf.

LII / Legal Information Institute. "18 U.S. Code § 2511 - Interception and Disclosure of Wire, Oral, or Electronic Communications Prohibited." Accessed January 25, 2020. https://www.law.cornell.edu/uscode/text/18/2511.

LII / Legal Information Institute. "18 U.S. Code Chapter 121 - Stored Wire and Electronic Communications and Transactional Records Access." Accessed January 25, 2020. https://www.law.cornell.edu/uscode/text/18/part-I/chapter-121.

LII / Legal Information Institute. "18 U.S. Code Chapter 206 - Pen Registers and Trap and Trace Devices." Accessed January 25, 2020. https://www.law.cornell.edu/uscode/text/18/part-II/chapter-206.

Ling, Justin. "Man Who Sold F-35 Secrets to China Pleads Guilty." *Vice* (blog), March 24, 2016. https://www.vice.com/en_us/article/kz9xgn/man-who-sold-f-35-secrets-to-china-pleads-guilty.

McGregor, Richard. "How the State Runs Business in China." *The Guardian*, July 25, 2019, sec. World news. https://www.theguardian.com/world/2019/jul/25/china-business-xi-jinping-communist-party-state-private-enterprise-huawei.

Milhaupt, Curtis J., and Wentong Zheng. "Beyond Ownership: State Capitalism and the Chinese Firm." *The Georgetown Law Journal,* 103 (n.d.): 59.

National Institute of Standards and Technology. "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1." Gaithersburg, MD: National Institute of Standards and Technology, April 16, 2018. https://doi.org/10.6028/NIST.CSWP.04162018.

NPR.org. "Charges Against Chinese Hackers Are Now Common. Why Don't They Deter Cyberattacks?" Accessed October 19, 2019. https://www.npr.org/2019/02/05/691403968/charges-against-chinese-hackers-are-now-common-why-dont-they-deter-cyberattacks.

"No Sign China Has Stopped Hacking U.S. Companies, Official Says - Bloomberg." Accessed September 2, 2019. https://www.bloomberg.com/news/articles/2015-11-18/no-sign-china-has-stopped-hacking-u-s-companies-official-says.

"ODNI_A_Guide_to_Cyber_Attribution.Pdf." Accessed September 22, 2019. https://www.dni.gov/files/CTIIC/documents/ODNI_A_Guide_to_Cyber_Attribution.pdf.

Pun, Darien. "Rethinking Espionage in the Modern Era." *Chicago Journal of International Law* 18, no. 1 (n.d.): 40.

Ravich, Samantha F., and Annie Fixler. "Framework and Terminology for Understanding Cyber-Enabled Economic Warfare," n.d., 18.

Recorded Future. "Threat Analyst Insights: The Impact of Indicting Foreign Nationals in Cyberespionage Cases," September 27, 2018. https://www.recordedfuture.com/foreign-cyberespionage-cases/.

"Rpt-China-Espionage.Pdf." Accessed September 2, 2019. https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf.

Sanger, David E. *The Perfect Weapon*. Crown Publishing, 2018.

Sciutto, Jim. "The Chinese Businessman Who Conned U.S. Defense Contractors." *The Daily Beast*, May 19, 2019, sec. arts-and-culture. https://www.thedailybeast.com/the-friendly-chinese-businessman-who-made-fools-of-us-defense-contractors.

Smith, Ms. "US Charges 3 Chinese Security Firm Hackers with Cyber Espionage." CSO Online, November 28, 2017. https://www.csoonline.com/article/3238828/us-charges-3-chinese-security-firm-hackers-with-corporate-cyber-espionage.html.

Spadafora, Anthony. "90 Percent of Data Breaches Are Caused by Human Error." TechRadar. Accessed November 3, 2019. https://www.techradar.com/news/90-percent-of-data-breaches-are-caused-by-human-error.

Telford, Taylor, "Marriott Discloses Massive Data Breach Affecting up to 500 Million Guests." Washington Post. Accessed October 14, 2019. https://www.washingtonpost.com/business/2018/11/30/marriott-discloses-massive-data-breach-impacting-million-guests/.

"The Real Reasons Why Cybercrimes Are Vastly Underreported." Accessed September 2, 2019. https://slate.com/technology/2018/02/the-real-reasons-why-cybercrimes-are-vastly-underreported.html.

"The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.Pdf." Accessed November 24, 2019. https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf.

"U.S. House of Representatives Committee on Oversight and Government Reform Report on the Equifax Data Breach." Accessed January 7, 2020. https://republicans-oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf.

"U.S.' Top Spy-Catcher: China Brings 'Ungodly Resources' to Espionage - CBS News." Accessed September 2, 2019. https://www.cbsnews.com/news/ncsc-director-says-china-is-the-largest-threat-to-national-security/.

"What Is a Zero Trust Architecture? - Palo Alto Networks." Accessed October 2, 2019. https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture.

"What Is a Zero Trust Architecture? - Palo Alto Networks." Accessed October 14, 2019. https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture.

War on the Rocks. "Cyber Attacks on Critical Infrastructure: Insights from War Gaming," July 26, 2017. https://warontherocks.com/2017/07/cyber-attacks-on-critical-infrastructure-insights-from-war-gaming/.

"What Is Data Masking? Data Masking Explained—BMC Blogs." Accessed October 2, 2019. https://www.bmc.com/blogs/data-masking/.

"What Is Data Masking? Data Masking Explained—BMC Blogs." Accessed October 14, 2019. https://www.bmc.com/blogs/data-masking/.

WhatIsMyIPAddress.com. "A VPN Masks Your Real IP Address. How It Does That Will Amaze You." Accessed November 1, 2019. https://whatismyipaddress.com/vpn-service.

Whitehouse.gov. "FACT SHEET: President Xi Jinping's State Visit to the United States," September 25, 2015. https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.

"Williams - The 'China, Inc.+' Challenge to Cyberspace Norms.Pdf." Accessed October 5, 2019. https://www.hoover.org/sites/default/files/research/docs/williams_webreadypdf1.pf.

"Wireshark · Go Deep." Accessed November 1, 2019. https://www.wireshark.org/.

World Economic Forum. "Explained, the Role of China's State-Owned Companies." Accessed October 4, 2019. https://www.weforum.org/agenda/2019/05/why-chinas-state-owned-companies-still-have-a-key-role-to-play/.

**National Security Fellows Program**
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 JFK Street
Cambridge, MA 02138

**www.belfercenter.org/NSF**



Printed in the United States of America