TAMING THE PAPER TIGER: DETERRING CHINESE ECONOMIC CYBER-ESPIONAGE AND REMEDIATING DAMAGE TO U.S. INTERESTS CAUSED BY SUCH ATTACKS

GRANT H. FRAZIER* & MARK B. FRAZIER†

ABSTRACT

The United States faces an increasingly complicated set of national security and economic threats. Chief among these are (1) progressively more sophisticated and damaging cyberattacks that threaten national security; harm government institutions, for-profit enterprises (including defense contractors), and institutions of higher learning; and undermine the country's system of property rights; and (2) rising levels of national debt held by foreign competitors.

China poses the greatest threat in both regards. China's government carries out, organizes, and/or facilitates cyberattacks to misappropriate intellectual property with serious consequences to the U.S.'s national security and economy. China also has acquired significant holdings in U.S. government-issued debt instruments. Mounting U.S. government debt restricts annual federal government budgetary decisions, negatively affects the U.S.'s international standing as a borrower, and threatens national security by giving foreign debt holders, such as China, potential leverage in foreign relations negotiations.

No policy prescription to date has achieved meaningful and lasting success in addressing these threats, and there are indications that the threats are only worsening. The National Trade Secret Protection and Remedy Strategy ("NTSPS") policy prescription proposed by this Article addresses the cyberattack and federal debt threats in a way that links and transforms them from vulnerabilities into leverage to protect the U.S.'s national security, system of property rights, and future economic well-being.

* Associate, Galbut Beabeau, P.C.; J.D., 2019, Sandra Day O'Connor College of Law at Arizona State University; B.S., 2016, Philosophy, Politics, and Economics, Pomona College. The author would like to thank his parents for their never-wavering love and support in all his pursuits—academic and otherwise. The policy prescription proposed in this paper is one of many that resulted from the authors' wonderful moral, political, philosophical, economic, and religious discussions when hiking the long-distance John Muir Trail in August–September 2019. John Muir said it best: "In every walk with Nature one receives far more than he seeks." Grant can be reached at: gfrazier@gb.law.

† Managing Partner, Rutan & Tucker, LLP; J.D., 1982, University of Southern California Gould School of Law; B.S., 1979, Diplomacy and World Affairs, Occidental College. The author would like to thank his son Grant for his love of family and family-endeavors, for developing the idea for this Article, for taking the laboring oar, and for the spirited policy debates we enjoyed during the writing process. Mark can be reached at: mfrazier@rutan.com.

Specifically, the U.S. government should pursue trade secret theft-related litigation and remedies against the Chinese government and its surrogates in U.S. federal courts. The proposed NTSPS would (1) create a specific, limited government property interest in intellectual property developed under government defense contracts; (2) create extra-territorial jurisdiction for the U.S. government and personal jurisdiction over foreign nations that engage in trade secret misappropriation either directly or indirectly through state-supported or enabled entities or persons; and (3) provide for readily available pre-judgment remedies, such as attachment and liens, to secure the government's remedy, and satisfaction of judgments through execution on U.S. debt held instruments held by the misappropriator—in this case, China. Successful implementation of the NTSPS would require amendments to several existing federal statutes and defense-contracting regulations and procedures.

Implementing the NTSPS strategy will allow the U.S. federal government to (1) compensate itself and U.S.-based companies for the damages each has suffered as the result of Chinese-led or -sponsored cyberattacks; (2) deter future Chinese cyberattacks by conveying a strong message that the U.S. will take meaningful action in response to said attacks; (3) slow the advancement of Chinese military technology by forcing China to internalize the significant research and development expenses incurred by the U.S. to develop the technological capabilities often targeted by cyber espionage initiatives; (4) significantly reduce U.S. debt and consequently the restrictions and burdens it places on the U.S. economy and national defense capability; and (5) pare down the financial leverage China holds over the U.S. in foreign relations.

INTRODUCTION

The U.S. is facing increasingly complicated and intertwined economic and national security threats. Chief among these are (1) increasingly pervasive cyberattacks on U.S. companies, government institutions, and universities to misappropriate intellectual property; and (2) mounting U.S. debt, especially to geopolitical and economic rivals, such as China.[1]

While China is by no means the only perpetrator of cyberattacks against the U.S. government and U.S.-based entities, China is, as further discussed herein, the worst perpetrator of these criminal acts and the greatest threat going forward. Chinese-organized or -sponsored cyberattacks to misappropriate intellectual property undermine the U.S.'s legal framework for the protection of property rights, cause significant monetary damages to intellectual property owners, and threaten the U.S.'s national defense and security by compromising the value of National Security Information.[2] While several U.S. administrations, including those

[1] Unless otherwise stated, the term "China" as used herein is meant to include China and Chinese governmental actors, as well as Chinese entities and nationals suspected to be aided and abetted by the Chinese government, or otherwise allowed by the Chinese government, to conduct cyberattack operations against U.S. interests.

[2] As used herein, "National Security Information" means information related to the national defense and foreign relations of the United States, which, if disclosed, could cause identifiable or describable damage to national security. *See generally* Exec. Order No. 13,526, 75 Fed. Reg. 707, 707 (Jan. 5, 2010). Such a definition is meant to be broad, encompass both political and economic relationships, and

led by Barack Obama[3] and Donald Trump,[4] have sought to deter cyberattacks by threatening increasingly harsh penalties, no policy prescription to date has proven to be effective.[5]

Also troubling are rising U.S. debt levels, which have skyrocketed since the Great Recession, and which have begun to weigh heavily on the U.S. federal government's annual budget and the nation's economy more generally.[6] This high national debt has additional negative consequences, including adversely affecting the U.S.'s international economic standing (most notably, as a borrower) and influence, as well as posing a threat to the U.S.'s national security.[7] The size of this debt is expected to grow, and it follows that the problems posed by the debt will increase in seriousness.[8] These preexisting risks have only been compounded by the COVID-19 pandemic, which has disrupted economic activity worldwide and spurred the U.S. government to implement several unprecedented stimulus packages, significantly increasing federal debt levels.[9]

Addressing these issues will require a multifaceted approach, including enabling legislation. Focusing on China, U.S.-based companies should pursue cyber-intellectual-property-theft-related litigation against Chinese companies engaged in misappropriation and/or the Chinese government if it facilitates or does not actively seek to prevent the misappropriation. Alternatively, U.S.-based companies should assign their litigation rights to

---

be in alignment with the Supreme Court's discussion of what constitutes "national defense"-related information. Gorin v. United States, 312 U.S. 19, 28 (1941) (holding that "national defense" is a "generic concept of broad connotations, referring to the military and naval establishments and the related activities of national preparedness"); United States v. Walli, 785 F.3d 1080, 1085 (6th Cir. 2015) (adopting the *Gorin* definition of "national defense" in the context of the Sabotage Act, which does not define the term); United States v. Platte, 401 F.3d 1176, 1190 (10th Cir. 2005) (adopting the same); United States v. Kabat, 797 F.2d 580, 586 (8th Cir. 1986) (adopting the same).

[3] Josh Rogin, *The Top 10 Chinese Cyber Attacks (That We Know Of)*, FOREIGN POL'Y (Jan. 22, 2010, 8:57 PM), https://foreignpolicy.com/2010/01/22/the-top-10-chinese-cyber-attacks-that-we-know-of/ [https://perma.cc/8YUQ-8JLW].

[4] Eric Geller, *U.S., Allies Slam China for Brazen Cyberattacks as Trump Administration Indicts Hackers*, POLITICO (Dec. 20, 2018, 10:42 AM), https://www.politico.com/story/2018/12/20/trump-administration-us-allies-condemn-china-for-brazen-cyberattacks-1070984 [https://perma.cc/7PVX-LCA8] ("DHS and the State Department warned Beijing to 'abide by its commitment to act responsibly in cyberspace' and said the U.S. would 'take appropriate measures to defend our interests.'").

[5] While the Trump administration has considered imposing sanctions on Chinese entities caught stealing U.S. IP through cyberattacks, no litigation-focused proposal of the type described herein has been proposed before. Jennifer Jacobs & Chris Strohm, *U.S. Planning Actions Targeting Chinese Hackers, Spies, Sources Say*, BLOOMBERG (Dec. 11, 2018, 5:02 PM), https://www.bloomberg.com/news/articles/2018-12-11/u-s-is-said-to-plan-actions-targeting-chinese-hackers-spies.

[6] Kimberly Amadeo, *US Debt to China, How Much It Is, Reasons Why, and What If China Sells*, BALANCE (Aug. 1, 2019), https://www.thebalance.com/u-s-debt-to-china-how-much-does-it-own-3306355 [https://perma.cc/CL95-HYCP].

[7] Vipal Monga, *High Debt Levels are Weighing on Economies*, WALL ST. J. (Sept. 8, 2019, 5:30 AM), https://www.wsj.com/articles/high-debt-levels-are-weighing-on-economies-11567935004?mod=e2tw [https://perma.cc/672H-7C59].

[8] *Id.*

[9] Russell Price, *COVID-19's Impact on the Government Debt Outlook*, AMERIPRISE FIN., https://www.ameripriseadvisors.com/team/cousino-moyer-group/insights/covid-19s-impact-on-the-government-debt-outlook (last visited July 24, 2020) (detailing how the federal policy actions taken since February 2020 to prop up the U.S. economy in the face of the COVID-19 pandemic, which include four stimulus bills, caused U.S. federal government debt to jump by $2.8 trillion, or about 16 percent. As of the end of April 2020, "[T]he Congressional Budget Office (CBO) now estimates a budget deficit of $3.7 trillion for fiscal 2020 (the federal fiscal year ends Sept. 30), and $2.1 trillion for fiscal 2021." The projected deficit may continue to swell. In March 2020, the CBO had projected a significantly lower deficit of approximately $1 trillion for both 2020 and 2021).

the U.S. government to pursue in order to provide deterrence to, and remedies for, misappropriation. Regardless of which of these avenues is utilized, the outcome is likely to be insufficient to accomplish these goals. Misaligned incentive structures, further discussed in Section V, do not encourage aggressive pursuit of claims, effective redress of harms, or deterrence of similar future misappropriations by international cybercriminals and their enablers.

Proper alignment of the incentive structure can be achieved via the U.S. government's enactment of the proposed NTSPS legislation. The NTSPS would provide the U.S. government with standing to pursue claims for misappropriation of any and all trade secrets that constitute National Security Information against China and other international actors under, among other things, the Economic Espionage Act of 1996,[10] the Defend Trade Secrets Act of 2016,[11] the Computer Fraud and Abuse Act,[12] and the National Stolen Property Act.[13]

The NTSPS would also provide for the following: (1) a pre-judgment attachment lien on U.S. debt instruments (e.g., Treasury notes) held by China's government and its surrogates when credible evidence exists of misappropriation by either principal or agent, and (2) direct execution on such notes to satisfy favorable judgments.

Implementing this strategy would allow the U.S. government to achieve several important policy goals, including (1) compensating U.S. companies and the U.S. federal government for the damages each has suffered as the result of past Chinese-led, -sponsored, or -allowed cyberattacks; (2) deterring future cyberattacks by conveying a strong message that the U.S. will take decisive action in response to said attacks; (3) reducing U.S. debt and the burdens it places on the U.S. economy and defense budget; and (4) reducing the financial leverage China holds over the U.S. in trade and foreign relations matters. However, such a course of action may expose the U.S. and U.S. companies doing business in China to a variety of retaliatory actions. A legal overview and related policy analysis of the effects of the proposed NTSPS policy prescription are provided below.

I. CHINA'S ONGOING CYBERATTACKS ON U.S. COMPANIES TO MISAPPROPRIATE INTELLECTUAL PROPERTY HAVE NATIONAL SECURITY AND ECONOMIC CONSEQUENCES

A. A TROUBLING, PERNICIOUS REALITY

China has been directly linked to cyberattacks on U.S. companies and government agencies for decades.[14] Experts estimate that China is

[10] Economic Espionage Act of 1996, 18 U.S.C. §§ 1831–39 (2018).

[11] Defend Trade Secrets Act of 2016, Pub. L. No. 114-153, 130 Stat. 376 (codified in scattered sections of 18 U.S.C.).

[12] Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2018).

[13] National Stolen Property Act, 18 U.S.C. §§ 2314–15 (2018).

[14] Geller, *supra* note 4 ("[P]rivate-sector cybersecurity researchers and U.S. intelligence officials have been saying for months: The 2015 agreement in which Beijing pledged to stop hacking U.S. companies for their valuable intellectual property is dead.").

responsible for over 90 percent of cyber espionage in the U.S., and between 50–80 percent of inter-border intellectual property theft worldwide.[15] In 2015, there was a glimmer of hope in the battle to decrease China's rampant cyberattack and theft efforts when the U.S. and China appeared to agree to not "conduct or knowingly support" cyber-theft of intellectual property or commercial trade secrets.[16] It appears this cyber-truce was relatively effective for a period of time after the 2015 agreement was finalized, as there was a dramatic decline in cyber breaches attributable to China during the final years of President Obama's tenure in office.[17] However, growing geopolitical and economic tensions[18] have led cybersecurity experts to note that the 2015 agreement is inoperative and that China has not adhered to it for years.[19] 2019 alone saw Chinese state-sponsored cyberattacks on a myriad of U.S. targets, including utilities,[20] cellular carriers,[21] cancer research institutes,[22] technology service providers,[23] and pharmaceutical companies,[24] among other industries.

China's cyberattacks take a significant economic toll on U.S. companies, with the estimated economic damage ranging from $200 billion

---

[15] *Report: Chinese Cyber Espionage Damaging U.S. Companies, National Security*, HOMELAND SEC. TODAY (Sept. 9, 2018), https://www.hstoday.us/subject-matter-areas/cybersecurity/report-chinese-cyber-espionage-damaging-u-s-companies-national-security/.

[16] Julianne Pepitone, *Obama: U.S. and China Reach Cyber-Espionage 'Common Understanding'*, NBC NEWS (Sept. 25, 2015, 9:36 AM), https://www.nbcnews.com/tech/security/obama-u-s-china-reach-cyber-spying-understanding-n433751.

[17] Joe Uchill, *Obama Administration Confirms Drop in Chinese Cyber Attacks*, HILL (June 27, 2016, 11:29 AM), https://thehill.com/policy/cybersecurity/285153-obama-administration-confirms-drop-in-chinese-cyber-attacks.

[18] Kevin Poulsen, *Obama's Cyberspace Peace with China is Just About Dead*, DAILY BEAST (Dec. 20, 2018, 5:44 PM), https://www.thedailybeast.com/obamas-cyberspace-peace-with-china-is-just-about-dead.

[19] *Id.* China has not materially adhered to the 2015 agreement since at least 2017. *See* Justin Lynch, *What Happens When the US-China Cyber Agreement Isn't Working,* FIFTH DOMAIN (Nov. 11, 2018), https://www.fifthdomain.com/international/2018/11/12/what-happens-when-the-us-china-cyber-agreement-isnt-working.

[20] Zak Doffman, *Chinese State Hackers Suspected of Malicious Cyber Attack on U.S. Utilities*, FORBES (Aug. 3, 2019, 2:31 AM), https://www.forbes.com/sites/zakdoffman/2019/08/03/chinese-state-hackers-suspected-of-malicious-cyber-attack-on-u-s-utilities/#4b13057e6758 ("The notorious Chinese state-sponsored hacking group APT10, which is believed to act for the country's Ministry of State Security, is the most likely culprit behind a cyber campaign targeting U.S. utility companies in July.").

[21] *Id.* ("[State-sponsored hacking group] APT10 made headlines in June, when it was reported that the group had compromised the systems of at least ten cellular carriers around the world to steal metadata related to specific users linked to China.").

[22] *Significant Cyber Incidents*, CTR. FOR STRATEGIC & INT'L STUD., https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents (last visited July 29, 2020).

[23] Jack Stubbs et al., *Exclusive: China Hacked Eight Major Computer Services Firms in Years-Long Attack*, REUTERS (June 26, 2019, 4:04 AM), https://www.reuters.com/article/us-china-cyber-cloudhopper-companies-exc/exclusive-china-hacked-eight-major-computer-services-firms-in-years-long-attack-idUSKCN1TR1D4 ("Hackers working for China's Ministry of State Security broke into networks of eight of the world's biggest technology service providers in an effort to steal commercial secrets from their clients, according to sources familiar with the attacks. . . . Reuters has found that at least six other technology service providers were compromised: Fujitsu, Tata Consultancy Services, NTT Data, Dimension Data, Computer Sciences Corporation and DXC Technology, HPE's spun-off services arm. Reuters has also identified more than a dozen victims who were clients of the service providers. That list includes . . . U.S. Navy shipbuilder Huntington Ingalls Industries . . . .").

[24] Pharmaceutical company Bayer announced that in April 2019 it had suffered an attempted cyberattack by Chinese hackers seeking to steal sensitive intellectual property. Jessica Davis, *Pharma Giant Bayer Targeted by Cyberattack, Threat Contained*, HEALTH IT SECURITY (Apr. 5, 2019), https://healthitsecurity.com/news/pharma-giant-bayer-targeted-by-cyberattack-threat-contained.

to $600 billion per year.[25] However, the damages caused by these cyberattacks are more than just monetary in nature. The theft and misappropriation of U.S. companies' intellectual property undermines the U.S.'s framework for the protection of property rights and legal system more generally, as well as threatens U.S. national security—especially in relation to cyberattacks on U.S. companies involved in the defense industry.[26]

Policy experts have noted the grave threat that China's cyberattacks on U.S. companies and government institutions pose to America's national security.[27] Even cyberattacks on U.S. universities have serious national defense implications. For example, a campaign of cyberattacks against twenty-seven universities across the U.S., Southeast Asia, and Canada targeted the schools' involvement in the research of various militaries' usage of maritime technology, with some of the schools being recipients of Navy defense contracts.[28]

II. THREATS OF FUTURE CYBERATTACKS TO MISAPPROPRIATE TRADE SECRETS ARE NOT ADEQUATELY MITIGATED BY THE U.S.-CHINA "PHASE ONE" TRADE DEAL OF JANUARY 2020

On January 15, 2020, the U.S. and Chinese governments agreed to the "Phase One" trade deal, which, among other things, included safeguards for intellectual property.[29] These safeguards include the following assurances: (1) U.S. companies may operate in China free of forced technology transfers; (2) China will seek to limit requests for information during licensing procedures;[30] and (3) certain protections for U.S. trade secrets will be honored, including China's prevention of "electronic intrusions"—a reference to computer hacking.[31]

While these safeguards may appear to address the above-described cyber espionage problem, this is unlikely to be the case. Policy experts have criticized the deal's provisions as not adding anything that was not already in place in previous U.S.-China agreements[32] and lacking the requisite specificity to achieve meaningful change.[33] For example, Harry G.

---

[25] Bill Gertz, *U.S. Hits Back Against Chinese Cyberattacks*, WASH. POST: INSIDE RING (Mar. 6, 2019), https://www.washingtontimes.com/news/2019/mar/6/us-counters-china-cyberattacks/.

[26] Rogin, *supra* note 3.

[27] Nicole Lindsey, *Chinese Cyber Threat Now Represents Threat to National Security, Say US Officials*, CPO MAG. (Nov. 15, 2019), https://www.cpomagazine.com/cyber-security/chinese-cyber-threat-now-represents-a-major-threat-to-national-security-say-us-officials/.

[28] Riley Walters & Michael Maher, *Why China's Intellectual Property Theft Is a Concern for National Security*, HERITAGE FOUND. (Apr. 4, 2019), https://www.heritage.org/asia/commentary/why-chinas-intellectual-property-theft-concern-national-security.

[29] Richard Altieri & Benjamin Della Rocca, *U.S. and China Sign "Phase One" Trade Deal but Leave Key Issues Unresolved*, LAWFARE (Jan. 22, 2020, 9:55 AM), https://www.lawfareblog.com/us-and-china-sign-phase-one-trade-deal-leave-key-issues-unresolved.

[30] *Id.*

[31] Peter Eavis et al., *What's in (and Not in) the U.S.-China Trade Deal*, N.Y. TIMES (Jan. 15, 2020), https://www.nytimes.com/2020/01/15/business/economy/china-trade-deal-text.html.

[32] Keith Johnson, *5 Takeaways from Trump's New China Trade Pact*, FOREIGN POL'Y (Jan. 16, 2020, 12:48 PM), https://foreignpolicy.com/2020/01/16/trump-new-china-trade-pact-takeaways/.

[33] Martha C. White, *Trump's China Deal Leaves Some Trade Experts 'Underwhelmed'*, NBC NEWS (Jan. 16, 2020, 4:59 PM), https://www.nbcnews.com/business/economy/trump-s-china-deal-leaves-some-trade-experts-underwhelmed-n1117471.

Broadman, Managing Director of the Berkeley Research Group and chair of the firm's emerging markets practice, noted, "On trade secrets, to be honest, the language that's in the agreement is pretty loose and generic . . . . On the face of it, I don't see — at least on that portion of the agreement — a lot that's significantly different from previous types of agreements."[34] Although China has agreed not to carry out, facilitate, or turn a blind eye to cyberattacks several times before, it has repeatedly violated its promises.

III. NATIONAL SECURITY CONSEQUENCES OF U.S. DEBT HELD BY CHINA

As of June 2020, the United States had over $26 trillion of debt.[35] A large portion of this debt—$19 trillion—is owned by the American people, domestically-based banks, or by the U.S. government itself.[36] However, several foreign nations are also large holders of U.S. debt. The most notable of these governmental debt holders is China, which currently holds $1.10 trillion of U.S. debt, down from its high holding point of $1.13 trillion of debt in 2013.[37] Governmental debt holders like China are willing to lend significant sums of money to the U.S. in return for continued U.S. consumption of the governmental debt holders' exports.

Geopolitical tensions between the U.S. and China have risen during President Trump's 2016–2020 term in office, as his administration has taken an increasingly firm stance on Chinese trade practices, among other government-supported or -facilitated policies.[38] Some commentators, including Chinese newspapers, have expressed concerns widely held by financial investors and analysts that China could use its $1.10 trillion of U.S. debt as a weapon to strike back at the U.S. in response to increased tariffs and other trade restrictions.[39]

National security concerns arising from Chinese misappropriation of trade secrets and Chinese holdings of U.S. debt instruments have not been adequately addressed in existing U.S. national security policy because they are not addressed as two elements of one cohesive, effective policy. Existing sovereign immunity protections unnecessarily and improperly immunize China and other international perpetrators of cyber espionage from trade secret theft liability. An effective trade secret enforcement

---

[34] *Id.*

[35] Bethany Blankley, *U.S. National Debt at Record $25 Trillion, Budget Deficit in April at $738 Billion*, CTR. SQUARE (May 15, 2020), https://www.thecentersquare.com/national/u-s-national-debt-at-record-25-trillion-budget-deficit-in-april-at-738-billion/article_1cd53d34-96c4-11ea-984e-4361912a1ea1.html.

[36] Amadeo, *supra* note 6.

[37] This decline in debt holding has been purposely facilitated by the Chinese government to "allow its currency, the yuan, to rise. To do that, China had to loosen its peg to the dollar. That made the yuan more attractive to forex traders in global markets." *Id.*

[38] *See, e.g.*, John Feffer, *The Widening Rift Between the US and China*, FOREIGN POL'Y (Apr. 8, 2019), https://www.thenation.com/article/china-us-xi-jinping-congagement/ ("And in a significant departure from its predecessor's version, the Trump administration's National Security Strategy portrays China as a 'revisionist' power that wants to 'shape a world antithetical to US values and interests.' This document 'suggests that wherever China is active, the United States should push back,' explains Melanie Hart, a China expert at the Center for American Progress.").

[39] Karen Yeung, *Will China Use its US$1.2 Trillion of US Debt as Firepower to Fight the Trade War?*, S. CHINA MORNING POST (May 10, 2019, 6:41 PM), https://www.scmp.com/economy/china-economy/article/3009752/will-china-use-its-us12-trillion-us-debt-firepower-fight.

mechanism, including deterrent and compensatory remedies, is necessary to adequately protect the U.S. and U.S. companies' respective intellectual property rights. The proposed NTSPS policy prescription includes use of existing substantive claims, suspension of sovereign immunity privileges, and ready access to U.S. debt instruments held by China or its surrogates as a source for such remedies.

IV. EXISTING LAWS PROVIDE ADEQUATE CLAIMS FOR TRADE SECRET MISAPPROPRIATION IF EXISTING STANDING, PERSONAL JURISDICTION, AND SOVEREIGN IMMUNITY LIMITATIONS ARE OVERCOME

State and federal law provide numerous statutory schemes to protect owners of trade secrets that qualify as National Security Information from misappropriation. Typically, such trade secret owners are private entities under contract with the U.S. government that create and use confidential information for national security purposes.[40] Such private entities may or may not have sufficient incentive or an available forum to seek redress from China for misappropriation, or may have economic disincentives to do so,[41] and are not well-positioned to pursue claims against China. Atypically, the U.S. government may be a co-owner or licensee of information developed by private companies that may constitute National Security Information.[42] Unfortunately, the government's lack of primary ownership or other right conferring standing to pursue claims for misappropriation of National Security Information limits the effectiveness of existing statutory claims and remedies to achieve U.S. economic and national security goals.

A. POTENTIAL CLAIMS BY U.S. COMPANIES

1. State Trade Secrets Laws

Trade secrets are forms of intellectual property, most often governed by state-level laws.[43] A trade secret may generally consist of any physical device, idea, pattern, formula, process, or compilation or information that (1) provides the owner of the trade secret with a competitive advantage in his/her/its respective marketplace; and (2) is protected in a way that can reasonably be expected to prevent the public or competitors from learning about the information's content, absent theft or other method of improper acquisition.[44] Examples of trade secrets include customer lists, cost and

[40] *See, e.g.*, Rick Richmond & Sandra Hanian, *Protecting Trade Secrets in Government Contracts*, 5 PRATT'S GOV'T CONTRACTING L. REP. 72 (2018).

[41] *See infra* Section V.

[42] *See* Susan B. Cassidy et al., *What Every Company Should Know About IP Rights When Selling to the US Government*, LANDSLIDE (July/Aug. 2017), https://www.americanbar.org/groups/intellectual_property_law/publications/landslide/2016-17/july-august/what-every-company-should-know-about-ip-rights-when-selling-us-government/ (discussing, among other things, the federal government's requirement of license agreements between a defense contractor and the government for certain types of technology).

[43] *Latest Updates on Federal Trade Secrets Legislation*, SEYFARTH SHAW https://www.tradesecretslaw.com/latest-update-on-federal-trade-secret-legislation/ [https://perma.cc/X4SE-2C5L] (last visited Nov. 1, 2020).

[44] *Id.*

pricing information, newly-created and not-yet-patented manufacturing techniques and processes, confidential information about business opportunities, and computer algorithms.[45] Trade secrets are protected at both the state[46] and federal levels. Because the Department of Justice ("DOJ") is the most likely prosecutor of the NTSPS discussed in this Article, the following analysis focuses on federal claims involving misappropriation of trade secrets that are National Security Information.

2. Federal Laws

a. Economic Espionage Act of 1996

The Economic Espionage Act of 1996 ("EEA") prohibits the "stealing, sharing, or receiving [of] a misappropriated trade secret."[47] Section 1881 addresses the theft of trade secrets for the benefit of a foreign government,[48] while Section 1832 addresses the theft of trade secrets generally.[49] A successful Section 1832 claim requires a showing of the defendant's "intent to convert a trade secret" and that the trade secret at issue is "related to or included in a product that is produced for or placed in interstate or foreign commerce."[50] Trade secrets underlying state-of-the-art military products that are sold to U.S. allies should meet the latter requirement, including Boeing's C-17 military transport aircraft and Lockheed Martin's F-22 and F-35 fighters—all of which have been targets of Chinese cyberattacks in recent years.[51]

The U.S. Attorney General is vested with the discretion to decide whether to prosecute violations of the EEA.[52] Structural and resource constraints imposed by the department's host of other prosecutorial

---

[45] *Id.*

[46] Most trade-secret-related litigation arises from protections provided by state law, and most of these state laws are similar in origin, with forty-eight out of the fifty United States having enacted a version of the Uniform Trade Secrets Act (UTSA). *Id.* The two states that have not enacted some version of the UTSA—New York and Massachusetts—protect trade secrets under the common law. *Id.* Many states have laws addressing hacking, malware, viruses, computer trespass, and unauthorized access. *See generally Computer Crime Statutes*, NAT'L CONF. ST. LEGISLATURES (Feb 24, 2020), http://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx. Depending on where the cyberattack is carried out, several state criminal statutes may also be implicated. *See, e.g.*, CAL. PENAL CODE § 499c (Deering 2020) (making it a crime to appropriate trade secrets by wrongful or dishonest means, or by conspiring or bribing anyone to do so); CAL. PENAL CODE § 496 (Deering 2020) (making it a crime to acquire or conceal property known to be stolen, with violations punishable by imprisonment and treble damages, costs, and attorneys' fees all available to the successful party under CAL. PENAL CODE § 496(c)); CAL. PENAL CODE § 502 (Deering 2020) (making it a crime to secure access to, and use, any computer hardware, software, or data without the authorization of the individual or entity that owns the hardware, software, or data).

[47] Economic Espionage Act of 1996, 18 U.S.C. §§ 1831, 1832 (2018); *see also* Steven Grimes & Shannon T. Murphy, *When to Call the Feds for Trade Secret Theft Investigations*, LAW360 (Feb. 5, 2019, 1:42 PM), https://www.law360.com/articles/1119887/when-to-call-the-feds-for-trade-secret-theft-investigations?te_pk=76785728-7d73-4440-8f0e-d5f4808b402b&utm_source=user-alerts&utm_medium=email&utm_campaign=tracked-entity-alert.

[48] *See* 18 U.S.C. § 1831.

[49] *See id.* § 1832.

[50] *See id.* § 1832(a).

[51] Jeff Daniels, *Chinese Theft of Sensitive US Military Technology is Still a 'Huge Problem,' Says Defense Analyst*, CNBC (Nov. 8, 2017, 10:26 PM), https://www.cnbc.com/2017/11/08/chinese-theft-of-sensitive-us-military-technology-still-huge-problem.html.

[52] *See* 18 U.S.C. § 1831.

responsibilities mean that the DOJ likely cannot pursue every instance of corporate trade secret theft committed or facilitated by China.

b. Defend Trade Secrets Act of 2016

The Defend Trade Secrets Act of 2016 ("DTSA"), which is codified at 18 U.S.C. § 1836, creates not only a criminal penalty, but also a private right of action in federal court for civil remedies to enjoin and compensate trade secret misappropriation.[53] The DTSA addresses misappropriation that manifests in several ways, including (1) "acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means," and (2) "disclosure" or "use of" another's trade secret without the consent of the trade secret owner.[54] In contrast to state trade secret laws, the DTSA applies to trade secret misappropriation that occurred before enactment of the DTSA as long as the misappropriation continues to occur after enactment of the DTSA.[55]

Remedies under the DTSA include pre-trial seizure of property necessary to prevent "propagation or dissemination of the trade secret,"[56] a tool not available in state variations of the Uniform Trade Secret Act ("UTSA"), as well as injunctive relief, compensatory and exemplary damages, and attorneys' fees.[57] The DTSA also provides civil and criminal immunity for whistleblowers.[58] Although the DTSA was enacted to replace the variations in state trade secret law that had arisen under the UTSA, the DTSA does not preempt state trade secret law and thus allows trade secret owners to pursue claims in either federal or state court and to combine DTSA and UTSA claims in one federal action if diversity jurisdiction exists.[59] Unfortunately, this flexibility leads to more complex and costly litigation. The ensuing jurisprudence has not resulted in uniform application of the DTSA. Federal courts searching for guidance in applying DTSA requirements have too frequently turned to state law decisions under the UTSA in their respective circuits, thereby grafting state law variations onto the DTSA.[60]

---

[53] *Id.* § 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.").

[54] *Id.* § 1839(5); *see, e.g.*, Brand Energy & Infrastructure Servs. v. Irex Contracting Grp., No. 16-2499, 2017 WL 1105648, at *3 (E.D. Pa. Mar. 24, 2017).

[55] Yeiser Research & Dev. LLC v. Teknor Apex Co., 281 F. Supp. 3d 1021, 1057 (S.D. Cal. 2017) (citing *Brand Energy & Infrastructure Servs.*, 2017 WL 1105648).

[56] 18 U.S.C. § 1836(b)(2)(A)(i) ("Application. Based on an affidavit or verified complaint satisfying the requirements of this paragraph, the court may, upon ex parte application but only in extraordinary circumstances, issue an order providing for the seizure of property necessary to prevent the propagation or dissemination of the trade secret that is the subject of the action.").

[57] *Id.* § 1836(b)(3).

[58] *See id.* § 1833(b); *see, e.g.*, Unum Grp. v. Loftus, 220 F. Supp. 3d 143, 146 (D. Mass. 2016); Christian v. Lannett Co., Inc., No. CV 16-963, 2018 WL 1532849, at *3 (E.D. Pa. Mar. 29, 2018).

[59] *See, e.g.*, *Yeiser Research & Dev. LLC*, 281 F. Supp. 3d at 1057 ("Importantly, the DTSA generally does not 'preempt or displace any other remedies, whether civil or criminal, provided by . . . State . . . law for the misappropriation of a trade secret…' 18 U.S.C. § 1838. Therefore, YRD may bring both a claim under the DUTSA and the DTSA."). *See generally* 18 U.S.C. § 1838.

[60] *See, e.g.*, Danielle A. Duszczyszyn & Daniel F. Roland, *Three Years Later: How the Defend Trade Secrets Act Complicated the Law Instead of Making It More Uniform*, FINNEGAN (July 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.

c. Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act ("CFAA") provides for both criminal prosecution and a private right of action in the event of certain unauthorized acts of access and/or damage to a protected computer.[61] Under the CFAA, "computer" means, with a few exceptions, any device that processes or stores data.[62] In addition to desktop and laptop computers, this definition includes restricted databases,[63] websites,[64] cell phones,[65] and iPads,[66] among other devices. However, not all "computers" under the statute are "protected computers." "Protected computers" means either computers (1) of the U.S. government, (2) of financial institutions, or (3) used in interstate or foreign commerce.[67] The broadest of these categories, and the most likely to apply in cases brought for trade secret misappropriation, involves computers used in interstate or foreign commerce. Courts have interpreted this category broadly to include any computer connected to the Internet.[68] The majority of computers used by defense companies will fall within this category. Even "air-gapped" computers—those isolated from unsecure networks (i.e., not directly connected to the Internet or any other system that is connected to the Internet)[69]—used by defense companies will likely constitute "protected computers" given their use in developing products for interstate and/or foreign commerce.

The seven classes of prohibited conduct that may give rise to a civil lawsuit are housed in 18 U.S.C. § 1030(a).

- Section 1030(a)(1) prohibits knowingly accessing a protected computer or exceeding authorized access to commit espionage;
- Section 1030(a)(2) prohibits intentionally hacking a protected computer and obtaining information that results in exposure to certain governmental, credit, financial, and/or computer-housed information;
- Section 1030(a)(3) prohibits unauthorized access of, or exceeding access to, of a government computer;
- Section 1030(a)(4) prohibits knowingly and, with intent to defraud, accessing a protected computer, without authorization or by exceeding authorized access, to obtain anything of value or further a fraud;
- Section 1030(a)(5) prohibits knowingly, intentionally, and without authorization causing damage to a government computer, bank computer, or a computer used in, or affecting,

[61] Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2018).
[62] *Id.* § 1030(e)(1).
[63] United States v. Valle, 807 F.3d 508, 513 (2d Cir. 2015).
[64] United States v. Drew, 259 F.R.D. 449, 457–58 (C.D. Cal. 2009).
[65] *See, e.g.*, United States v. Nosal, 844 F.3d 1024, 1050–51 n.3 (9th Cir. 2016); *see also* United States v. Mitra, 405 F.3d 492, 495 (7th Cir. 2005).
[66] United States v. Nosal, 676 F.3d 854, 861 (9th Cir. 2012).
[67] 18 U.S.C. § 1030(e)(2).
[68] *See, e.g.*, *Nosal*, 676 F.3d at 859; United States v. Trotter, 478 F.3d 918, 921 (8th Cir. 2007).
[69] *See* Max Eddy, *Black Hat Researcher Shows Why Air Gaps Won't Protect Your Data*, PC MAG (Aug. 9, 2018), https://www.pcmag.com/news/black-hat-researcher-shows-why-air-gaps-wont-protect-your-data. Air-gapped computers are most often utilized by military organizations and governments. *Id.*

interstate or foreign commerce (*e.g.*, via a computer virus, Trojan horse, etc.);

- Section 1030(a)(6) prohibits the knowing and intentional trafficking of passwords for a government computer when the trafficking affects interstate or foreign commerce; and
- Section 1030(a)(7) prohibits threats, made with intent to extort, to damage a government computer, bank computer, or computer used in, or affecting, interstate or foreign commerce.[70]

It is clear that the CFAA prohibits an individual from accessing a computer that they are not authorized to access under any circumstances. What is less clear is whether the CFAA applies to an individual who has accessed electronic information in excess of some preexisting, limited authorization. The federal circuit courts are split on this point.[71] It appears the U.S. Supreme Court is ready to resolve the circuit split, announcing it would hear the Eleventh Circuit case *United States v. Van Buren* during the October 2020 term.[72]

Specifically, to bring a civil action, the complained-of conduct must include one of the following factors:

1) loss to one or more persons during any one-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting one or more other protected computers) aggregating at least five thousand dollars in value;
2) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of one or more individuals;
3) physical injury to any person;
4) a threat to public health or safety; or
5) damage affecting a computer used by or for an entity of the United States government in furtherance of the administration of justice, national defense, or national security[73]

Such lawsuits must be brought within two years of the complained-of act or within two years of when the resulting damage is discovered.[74]

---

[70] *See* 18 U.S.C. § 1030(a)(1)–(7).

[71] Alan R. Friedman et al., *Supreme Court to Resolve Circuit Split Regarding the Scope of the Computer Fraud and Abuse Act, Which Has Been Used to Prosecute Alleged Unauthorized-Use Crimes*, KRAMER LEVIN (Apr. 22, 2020), https://www.kramerlevin.com/en/perspectives-search/supreme-court-to-resolve-circuit-split-regarding-the-scope-of-the-computer-fraud-and-abuse-act-which-has-been-used-to-prosecute-alleged-unauthorized-use-crimes.html ("To date, seven circuit courts have weighed in on the scope of the CFAA. The First, Fifth, Seventh and Eleventh Circuits have broadly interpreted the statutory meaning of accessing information 'in excess of authorization' and criminalized access to a computer (use that is otherwise authorized) when that occurred for an improper purpose. In contrast, the Second, Fourth and Ninth Circuits have narrowly interpreted the CFAA, holding that a defendant violates the statute only if she is prohibited from accessing the computer under all circumstances."). For example, a current or former employee who copies company files that the employee is prohibited from accessing could be liable for exceeding their access in violation of the CFAA. *Id.*

[72] *Id.*

[73] *See* 18 U.S.C. § 1030(g).

[74] *See id.*

Successful plaintiffs may obtain compensatory damages, which are statutorily limited to economic damages.[75] Other equitable relief, including injunctive relief, is also available.[76]

The EEA, DTSA, and CFAA provide U.S. companies with avenues to remedy the cybertheft of National Security Information, but for reasons discussed in Section V below, companies may face legal and economic obstacles and disincentives to obtaining redress for such theft. As a more effective alternative, the U.S. government may pursue redress under existing statutes and regulations as modified by the NTSPS.

B. POTENTIAL CLAIMS BY THE U.S. GOVERNMENT

Whether the U.S. government has standing to bring claims under the EEA, DTSA, or CFAA for misappropriation of National Security Information depends on ownership in the misappropriated information. If a U.S. company is the sole owner of the National Security Information, the U.S. government lacks standing to bring claims. If, however, the U.S. government is the owner or a co-owner of the information, standing will exist to pursue the claims. This may even be true in situations in which the U.S. government is a licensee.[77] In any event, the U.S. government may bring the following criminal actions with criminal penalties for misappropriation.

1. Computer Fraud and Abuse Act

The CFAA, discussed above in connection with its civil provisions, also provides for criminal prosecution.[78] Specifically, it protects federal computers, bank computers, and computers connected to the Internet.[79] The CFAA attempts to safeguard them from trespassing, threats, damage, espionage, and from being corruptly used as instruments of fraud.[80] A violation of 18 U.S.C. § 1030 requires the following elements to be met: (1) knowingly accessing a protected computer without authorization or in excess of authorization; (2) obtaining national security information; (3) with reason to believe the information could injure the U.S. or benefit a

---

[75] *Id.*

[76] *Id.*

[77] *See* Cassidy et al., *supra* note 42 (discussing the federal government's requirement of license agreements between it and defense contractors for certain types of technology). Federal trade secrets law allows licensees to sue, sometimes explicitly. DTM Research, L.L.C. v. AT&T Corp., 245 F.3d 327, 332 (4th Cir. 2001) (holding that a non-exclusive licensee nonetheless had standing to sue for misappropriation of the trade secret). The DTSA goes so far as to make this explicit in providing: "an *owner* of a trade secret that is misappropriated may bring a civil action," 18 U.S.C. § 1836 (emphasis added), with "owner" defined to include the "person or entity in whom or in which rightful legal or equitable title to, *or license in*, the trade secret is reposed." 18 U.S.C. § 1839(4) (emphasis added). State trade secret laws have also been interpreted to authorize trade secret misappropriation suits by licensees. *See, e.g.*, Advanced Fluid Sys. v. Huber, 28 F. Supp. 3d 306, 319 n.4, 323 (M.D. Pa. 2014) (holding that "ownership, in the traditional sense, is not prerequisite" to bringing a trade secret misappropriation claim); Metso Minerals Indus. V. FLSmidth-Excel, 733 F. Supp. 2d 969, 977–79, 977 n.12 (E.D. Wis. 2010) (holding that a non-exclusive licensee could pursue a trade secret misappropriation claim).

[78] *See generally* COMPUT. CRIME & INTELL. PROP. SECTION CRIM. DIV., PROSECUTING COMPUTER CRIMES (2010), https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf [https://perma.cc/7YGE-X6NC].

[79] 18 U.S.C. § 1030(e)(2).

[80] *See generally* 18 U.S.C. § 1030.

foreign nation; and (4) in order to willfully communicate, deliver, or transmit the information (or attempt to do so) or willfully retain the information.[81]

For purposes of the CFAA, national security information means information that has "been determined by the United States government pursuant to an Executive Order or statute to require protection from unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954."[82] This definition falls within National Security Information as used in this Article. Convictions are felonies punishable by fines and imprisonment for not more than ten years for an initial violation, and imprisonment for not more than twenty years for a subsequent violation.[83] An eight-year statute of limitations applies to crimes under Section 1030(a)(1), except there is no statute of limitations for crimes that create a foreseeable risk of serious bodily injury or death to another person.[84] An example of such a crime may be the theft or corruption of COVID-19-related vaccination testing information, which could delay deployment of an effective vaccination, thereby leading to illness and death.[85]

2. Mail and Wire Fraud

18 U.S.C. §§ 1341 and 1343 prohibit schemes to defraud or obtain money or other property by false or fraudulent pretenses via use of the United States Postal Service for mail fraud; or wire, radio or television communications for wire fraud. Following similar reasoning to the above, trade secrets and other confidential information qualify as "property" under 18 U.S.C. §§ 1341 and 1343.

Mail fraud occurs when a person (1) devises or intends to devise a scheme to defraud or to perform specific fraudulent acts; and (2) uses the mail for the purpose of executing or attempting to execute the scheme, or performs specified fraudulent acts.[86] The crime of wire fraud parallels the crime of mail fraud, except that wire fraud concerns communications transmitted by wire.[87] The statute of limitations for mail and wire fraud is five years,[88] unless the fraud involves a financial institution, in which case the limitations period is ten years.[89]

Punishments for violations of the mail and wire fraud statutes are significant. An individual who has violated one of the laws will be subject to either up to five years in prison or a fine of up to $250,000,[90] or both.

---

[81] *See generally id.*
[82] *Id.* § 1030(a).
[83] *Id.* § 1030(c)(1)(A)–(B).
[84] *See generally* COMPUT. CRIME & INTELL. PROP. SECTION CRIM. DIV., *supra* note 78.
[85] This is not an implausible worry. *See, e.g.*, Ellen Nakashima & Devlin Barrett, *U.S. Accuses China of Sponsoring Criminal Hackers Targeting Coronavirus Vaccine Research*, WASH. POST (July 21, 2020, 11:46 AM), https://www.washingtonpost.com/national-security/us-china-covid-19-vaccine-research/2020/07/21/8b6ca0c0-cb58-11ea-91f1-28aca4d833a0_story.html.
[86] Schmuck v. United States, 489 U.S. 705, 721 n.10 (1989).
[87] United States v. Frey, 42 F.3d 795, 797 (3rd Cir. 1994).
[88] 18 U.S.C § 3282 .
[89] *Id.* § 3293.
[90] *Id.* §§ 1341, 1343.

Because these statutes define elements of a crime that are easier to prove than the elements under the Economic Espionage Act of 1996, federal prosecutors may prefer to prosecute a trade secrets case involving National Security Information under the mail and wire fraud statutes.

3. The National Stolen Property Act

The National Stolen Property Act (NSPA), located at 18 U.S.C. § 2314, prohibits the receipt, sale, or transportation of interstate or foreign commerce involving stolen "goods, wares, merchandise, securities or money, of the value of $5,000 or more." Department of Justice lawyers bringing suit against China could argue that the stolen and/or misappropriated intellectual property constituting National Security Information qualifies as "goods, wares, [or] merchandise," and as long as the value of the stolen and/or misappropriated intellectual property exceeds the five thousand dollar statutory minimum, the NSPA applies. Should a violation of the NSPA be found, such violation is punishable by either a fine of up to $250,000 or imprisonment of up to ten years, or both.[91]

C. FOREIGN SOVEREIGN IMMUNITIES ACT—A MAJOR OBSTACLE TO BRINGING CLAIMS IN U.S. COURTS FOR CHINESE MISAPPROPRIATION OF U.S. TRADE SECRETS

Misappropriated trade secrets are typically owned by U.S. private companies, which include defense contractors such as Lockheed Martin, Boeing, Raytheon, Northrop Grumman, and General Dynamics.[92] As owners of the misappropriated trade secrets, these private companies have standing to bring claims. They may, however, lack incentive to bring such claims.[93] Atypically, the U.S. government is the trade secret owner. A serious weakness in the existing fabric of trade secret laws is lack of clear government ownership of misappropriated trade secrets that constitute confidential National Security Information.

U.S. laws do not, as a general rule, apply outside the United States unless Congress expresses a clear intent otherwise.[94] Extraterritorial jurisdiction, and its reach, are determined on a statute-by-statute basis based on Congressional intent.[95] Both the EEA and its DTSA amendment provide for extra-territorial application if an act in furtherance of the offense is committed in the U.S., or if the offender was, at the time of the act, a U.S. citizen or permanent resident.[96] Lacking, however, is express intent to apply the statutes to a foreign government acting entirely outside the U.S. territorial jurisdiction.

---

[91] *Id.* § 3571.

[92] *See, e.g.*, Daniels, *supra* note 51 (discussing Chinese theft of trade secrets from U.S. defense companies, including Lockheed Martin and Boeing).

[93] *See generally infra* Section V.

[94] *See* Morrison v. Nat'l Australia Bank Ltd., 561 U.S. 247 (2010).

[95] *Id.* at 255 ("Legislation of Congress, unless a contrary intent appears, is meant to apply only within the territorial jurisdiction of the United States.").

[96] United States v. Kolon Indus., Inc., 926 F.Supp.2d 794, 802 (E.D. Va. 2013) ("In enacting the trade secret statutes . . . Congress plainly provided that their terms are applicable to foreign defendants where 'an act in furtherance of the offense was committed in the United States.'" (quoting 18 U.S.C. § 1837(2))).

The problems created by limited resort and access to U.S. courts are exacerbated by immunity defenses that unnecessarily shield China from the consequences of its wrongful actions.

1. Foreign Sovereign Immunities Act

Generally recognized principles of sovereign immunity dictate that a foreign sovereign ("Sovereign A") cannot be sued in another sovereign's ("Sovereign B") courts without Sovereign A's consent.[97] This concept is known in international law as the State Immunity Doctrine,[98] and it serves to recognize each state's equal right to independence.[99] The U.S. has a long tradition of following this doctrine by maintaining that private parties cannot sue sovereigns, except in very limited circumstances. Notably, the Supreme Court in *The Schooner Exchange v. M'Faddon* effectively held that the State Immunity Doctrine granted foreign sovereign states absolute immunity from U.S. jurisdiction absent the state's implied or explicit consent.[100] From the time *Schooner Exchange* was decided in 1812 until the mid-twentieth century, lower U.S. courts adhered to this ruling, refusing to hear claims against foreign sovereigns based on common law principles, even when the claims being brought related to commercial activities.[101] As part of this deferential decision-making process, courts often relied on suggestions of immunity by the U.S. State Department.[102] These suggestions took a more formal form in 1952 with the U.S. State Department's adoption of the Restrictive Theory of Sovereign Immunity, which held that generally public acts of a foreign state are entitled to immunity, while private acts are not.[103]

With the passage of the Foreign Sovereign Immunities Act ("FSIA") in 1976,[104] the U.S. became the first nation to codify the law of sovereign immunity via statute.[105] The FSIA "provides the sole basis for obtaining

[97] *See, e.g.*, GARY B. BORN & DAVID WESTIN, INTERNATIONAL CIVIL LITIGATION IN UNITED STATES COURTS 335 & n.1 (1989); LUNG CHU CHEN, AN INTRODUCTION TO CONTEMPORARY INTERNATIONAL LAW 242 (1989); MALCOLM N. SHAW, INTERNATIONAL LAW 431 (3d ed. 1991); Thomas H. Hill, *A Policy Analysis of the American Law of Foreign State Immunity*, 50 FORDHAM L. REV. 155, 158 (1981).

[98] For more on the State Immunity Doctrine, see generally William Baude, *Sovereign Immunity and the Constitutional Text*, 103 VA. L. REV. 1 (2017).

[99] *See generally* Miles McCann, *State Sovereign Immunity*, 2 NAGTRI J. 12, 13 (2017).

[100] Schooner Exchange v. McFaddon, 11 U.S. 116, 147 (1812).

[101] Haim Abraham, *Awarding Punitive Damages Against Foreign States is Dangerous and Counterproductive*, LAWFARE (Mar. 1, 2019, 8:00AM), https://www.lawfareblog.com/awarding-punitive-damages-against-foreign-states-dangerous-and-counterproductive.

[102] Saudi Arabia v. Nelson, 507 U.S. 349, 362 n.5 (1993) ("Prior to the Act's passage, the State Department would determine in the first instance whether a foreign state was entitled to immunity and make an appropriate recommendation to the courts.") (citing Verlinden B.V. v. Cent. Bank of Nigeria, 461 U.S. 480, 486–88 (1983)).

[103] Jack B. Tate, *Changed Policy Concerning the Granting of Sovereign Immunity to Foreign Governments*, 26 DEP'T ST. BULL. 984, 985 (1952) [hereinafter, the "Tate Letter"] (advising the Justice Department that from then on, the State Department would "follow the restrictive theory of sovereign immunity in the consideration of requests of foreign governments for a grant of sovereign immunity."); *see, e.g.*, Alfred Dunhill, Inc. v. Cuba, 425 U.S. 682, 711–15 (1976) (quoting the Tate Letter in discussing the same); *see also* William W. Bishop, Jr., *New United States Policy Limiting Sovereign Immunity*, 47 AM. J. INT'L L. 93, 104–06 (1953) (commenting on the U.S. State Department's adoption of the restrictive doctrine of sovereign immunity).

[104] Codified at 28 U.S.C. §§ 1330, 1332, 1391(F), 1441(d), 1602–11 (2018).

[105] Mark B. Feldman, *The United States Foreign Sovereign Immunities Act of 1976 in Perspective: A Founder's View*, 35 INT'L & COMP. L.Q. 302, 303 (1986); *see also* Verlinden B.V., 461 U.S. at 487–88 (holding that the FSIA "codifies, as a matter of federal law, the restrictive theory of sovereign immunity," under which "immunity is confined to suits involving the foreign sovereign's public acts,

jurisdiction over a foreign state" in U.S. courts.[106] The FSIA also establishes specific procedures for technical aspects of suits that are allowed under the FSIA, including service of process,[107] attachment of property,[108] and execution of judgment in proceedings against a foreign state.[109]

Under the FSIA, "a foreign state is presumptively immune from the jurisdiction of United States courts; unless a specified exception applies, a federal court lacks subject-matter jurisdiction over a claim against a foreign state."[110] 28 U.S.C. § 1605 contains several important exceptions to the FSIA's default of sovereign immunity. If one or more of these exceptions applies, then a court that would otherwise have subject matter jurisdiction, if it were not for the FSIA, may exercise such jurisdiction. The applicability of the exceptions most relevant to the China-conducted and/or -facilitated cyber espionage are discussed below.

2. Relevant Exceptions to the FSIA

a. Commercial Activity Exception

The Supreme Court has held that "Foreign sovereigns (unlike States) are generally not immune from suits arising from their commercial activities."[111] In so doing, the Court relies on the "Commercial Activity Exception" to the FSIA, which provides the following:

> A foreign state shall not be immune from the jurisdiction of courts of the United States or the States in any case . . . in which the action is based upon a commercial activity carried on in the United States by the foreign state; or upon an act performed in the United States in connection with a commercial activity of the foreign state elsewhere; or upon an act outside the territory of the United States in connection with a commercial activity of the foreign state elsewhere and that act causes a direct effect in the United States.[112]

The Commercial Activity Exception essentially codified the Tate Letter—a predating U.S. State Department document outlining the commercial activity policy[113]—and requires a reviewing court to determine

---

and does not extend to cases arising out of a foreign state's strictly commercial acts."). The three broad objectives of this set of statutes are: "(1) to transfer responsibility for immunity determinations from the Department of State to the judiciary; (2) to define and codify the 'restrictive' theory of immunity; and (3) to provide a comprehensive, uniform regime for litigation against foreign states and governmental agencies." Feldman, *supra* at 303.

[106] *Saudi Arabia*, 507 U.S. at 355 (quoting Argentine Republic v. Amerada Hess Shipping Corp., 488 U.S. 428, 443 (1989)).

[107] *See* 28 U.S.C. § 1608 (2018).

[108] *Id.* § 1609 (providing that foreign sovereigns are immune from, inter alia, attachment, except as provided by 28 U.S.C. §§ 1610-11); *Id.* § 1610 (stating the exceptions to the general immunity from attachment provided in 28 U.S.C. § 1609).

[109] *Id.* § 1610.

[110] *Saudi Arabia*, 507 U.S. at 355 (citation omitted).

[111] Michigan v. Bay Mills Indian Cmty., 572 U.S. 782, 804 (2014) (citing 28 U.S.C. § 1605(a)(2)).

[112] 28 U.S.C. § 1605(a)(2).

[113] *Bay Mills Indian Cmty.*, 572 U.S. at 801 n.10 ("*Kiowa* explained that Congress, in the Foreign Sovereign Immunities Act of 1976, 28 U.S.C. § 1605(a)(2), 'den[ied] immunity for the commercial acts

whether the sovereign's actions at issue are commercial in nature.[114] The test does not consider the foreign state's purpose or motives, but rather hinges on whether the conduct is the type which private parties usually engage in for "trade and traffic or commerce."[115] For example, the U.S. Supreme Court in *Republic of Argentina v. Weltover, Inc.* held that Argentina's refinancing of debt via bond issuance constituted a "commercial activity" under the FSIA because Argentina participated in the bond market not as a regulator, but in the manner of a private player within the market.[116]

However, the Commercial Activity Exception contains a loophole that allows foreign sovereigns to escape U.S. jurisdiction by masking the sovereign's commercial activity as otherwise sovereign activities of one of its state agencies. The Supreme Court opinion in *Saudi Arabia v. Nelson* highlights this loophole.[117] In *Saudi Arabia*, the Supreme Court noted that "where a claim rests entirely upon activities sovereign in character . . . jurisdiction will not exist under that clause [(the Commercial Activity Exception)] regardless of any connection the sovereign acts may have with commercial activity."[118] The Court held that Saudi Arabia's alleged wrongful arrest, imprisonment, and torture of an American citizen employed at a Saudi hospital did not constitute a "commercial activity," but rather fell under the country's police power—a power peculiar to sovereigns.[119] This loophole has been limited in situations in which the sovereign is both carrying out a traditional sovereign activity and also engaging in commercial activity. Notably, the Commercial Activity Exception has been met even in cases involving actions traditionally undertaken by sovereigns—such as large-scale transformation of economic systems (e.g., communist to free market)[120] and management and regulation of nuclear power.[121]

China's ordering, facilitating, or turning a blind eye to cyberattacks to misappropriate U.S. trade secrets involves commercial activity rather than the exercise of police power and hence falls within the "commercial activity" exception.

---

of a foreign nation,' codifying an earlier State Department document, known as the Tate Letter, announcing that policy." (citing Kiowa Tribe of Okla. v. Mfg. Techs., 523 U.S. 751, 759 (1998))).

[114] *See* 28 U.S.C. § 1603(d); Republic of Argentina v. Weltover, Inc., 504 U.S. 607, 614 (1992).

[115] *Weltover, Inc.*, 504 U.S. at 614 (citation omitted).

[116] *Id.*

[117] *See* Saudi Arabia v. Nelson, 507 U.S. 349 (1993).

[118] *Id.* at 358 n.4.

[119] *Id.* at 361.

[120] WMW Machinery, Inc. v. Werkzeugmaschinenhandel GmbH Im Aufbau, 960 F. Supp. 734, 740 (S.D.N.Y. 1997) (holding the German government's alleged tortious interreference with the plaintiff's pre-existing manufactured goods distribution rights was "commercial" under the FSIA, despite the government's stated sovereign purpose of converting state-owned businesses in formerly East Germany into free market enterprises).

[121] Lantheus Med. Imaging, Inc. v. Zurich Am. Ins. Co., 841 F. Supp. 2d 769, 788–89 (S.D.N.Y. 2012) (holding that a state-owned Canadian corporation—which operated a nuclear reactor, marketed itself as a commercial enterprise, and supplied a large portion of the worldwide need for medical isotopes—was commercial in nature under the FSIA).

b. Explicit or Implicit Waiver of Immunity

Sovereign immunity may be deemed to have been explicitly or implicitly waived by a sovereign's conduct. 28 U.S.C. § 1605(a)(1) provides the following:

> A foreign state shall not be immune from the jurisdiction of courts of the United States or the States in any case . . . *in which the foreign state has waived its immunity* either *explicitly* or *by implication*, notwithstanding any withdrawal of the waiver which the foreign state may purport to effect except in accordance with the terms of the waiver.[122]

In general, courts are extremely hesitant to find that a foreign sovereign has implicitly waived its immunity.[123] However, courts have done so in one of three situations: (1) when a foreign sovereign agrees to arbitration in another country; (2) when a foreign sovereign agrees that the laws of another country govern a contract; or (3) when a foreign sovereign files a responsive pleading without raising the immunity defense.[124]

The second and third situations are unlikely to occur. The first situation may occur in the context of the Chinese government (or one of its state-owned entities implicated in the hypothetical cyberattack) agreeing to a contract with a U.S. company involved in the defense industry. If this contract contains a dispute resolution provision providing for arbitration in the U.S., the U.S. company may be able to utilize the FSIA exception in 28 U.S.C. § 1605(a)(1). It is, however, unlikely that China, or one of its state-owned entities, would agree to such an arbitration provision.

c. Expropriation Exception

The defense of sovereign immunity may be defeated via the Expropriation Exception, located at 28 U.S.C. § 1605(a)(3), which provides the following:

> A foreign state shall not be immune from the jurisdiction of courts of the United States or the States in any case . . . in which rights in property taken in violation of international law are in issue and that property or any property exchanged for such property is present in the United States in connection with a commercial activity carried on in the United States by the foreign state. . . .[125]

The Supreme Court has held the Expropriation Exception is satisfied if "(1) 'rights in property taken in violation of international law are in issue,'

---

[122] 28 U.S.C. § 1605(a)(1) (emphasis added).

[123] Coleman v. Alcolac, Inc., 888 F. Supp. 1388, 1397 (S.D. Tex. 1995) ("The implicit waiver clause of 1605(a)(1) has been very narrowly construed. Courts have shown great reluctance to stray beyond the[] [provided] three examples of implicit waiver. Courts will rarely find that a nation has waived its sovereign immunity without strong evidence that waiver was what the state intended." (citations omitted)).

[124] Gutch v. Fed. Republic of Germany, 444 F. Supp. 2d 1, 5 (D.D.C. 2006), *aff'd*, 255 F. App'x 524 (D.C. Cir. 2007).

[125] 28 U.S.C. 1605(a)(3).

and (2) there is an adequate commercial nexus between the United States and the defendants."[126]

Courts have interpreted "taken," which is not defined in the FSIA, to mean a foreign sovereign's nationalization or expropriation of property without payment of prompt, adequate, and effective compensation as required by international law.[127] In the case of 28 U.S.C. § 1605(a)(3), "international law" does not refer to bodies of international law, like human rights laws, but rather is a reference to the international law of expropriation and state responsibility.[128] As provided by the court in *de Csepel v. Republic of Hungary*, a taking violates international law if: "(1) it was not for a public purpose, (2) it was discriminatory, or (3) no just compensation was provided for the property taken."[129]

Misappropriation by cyberattack as described in this Article should satisfy each of the tests in *de Csepel*. Such a situation involves rights in trade secrets (via direct ownership or as a licensee); a violation of international law via, among other things, an unlikelihood that just compensation was provided for the misappropriated property; and a strong commercial nexus existing between the United States and China.[130]

d. Non-Commercial Tort Exception

At first blush, it appears China's sovereign immunity defense may also be defeated via the Non-Commercial Tort Exception, located at 28 U.S.C. § 1605(a)(5), which provides:

> A foreign state shall not be immune from the jurisdiction of courts of the United States or the States in any case . . . not otherwise

---

[126] de Csepel v. Republic of Hung., 859 F.3d 1094, 1101 (D.C. Cir. 2017) (citing Agudas Chasidei Chabadof U.S. v. Russian Federation, 528 F.3d 934, 940 (D.C. Cir. 2008)).

[127] *See* Zappia Middle E. Constr. Co. v. Emirate of Abu Dhabi, 215 F.3d 247, 251 (2d Cir. 2000) ("[T]he legislative history makes clear that the phrase 'taken in violation of international law' refers to 'the nationalization or expropriation of property without payment of the prompt, adequate and effective compensation required by international law,' including 'takings which are arbitrary or discriminatory in nature'" (quoting H.R. Rep. No. 94-1487, at 19 (1976), *as reprinted in* 1976 U.S.C.C.A.N. 6004, 6618)).

[128] Kalamazoo Spice Extraction Co. v. Provincial Military Gov't of Socialist Ethiopia, 729 F.2d 422, 425–26 (6th Cir. 1984) (allowing a 28 U.S.C. § 1605(a)(3) expropriation claim to proceed based on alleged violations of a bilateral treaty of friendship, commerce, and navigation); *see also* McKesson Corp. v. Islamic Republic of Iran, Civ. Action No. 82-0220 (RJL), 2009 WL 4250767, at *3–4 (D.D.C. Nov. 23, 2009) (holding that the FSIA's commercial activities exception permits a plaintiff to base an expropriation claim on customary international law).

[129] de Csepel v. Republic of Hung., No. 1:10-CV-01261(ESH), 2020 WL 2343405, at *19 (D.D.C. May 11, 2020) (quoting de Csepel v. Republic of Hungary, 808 F. Supp. 2d 113, 128 (D.D.C. 2011), *aff'd in part,* 714 F.3d 591 (D.C. Cir. 2013)).

[130] The targeted trade secrets, by their very definition, hold commercial value; the access point of the cyber breach would be U.S. based servers; and the resulting harm would be suffered in the U.S. *See, e.g.*, Vermont Microsystems, Inc. v. Autodesk, Inc., 88 F.3d 142, 149 (2d Cir. 1996) (quoting CAL. CIV. CODE § 3426.1(d)(1)) (discussing how California law affords protection only to those trade secrets which meet a two-part definition: (1) subject to reasonable measures to ensure the trade secrets' secrecy, and (2) trade secrets also must "[d]erive [] independent economic value, actual or potential, from not being generally known to the public or to other persons who can obtain economic value from [their] disclosure or use."); *see also* Religious Tech. Ctr. v. Wollersheim, 796 F.2d 1076, 1090 (9th Cir. 1986). *But see* Learning Curve Toys, Inc. v. PlayWood Toys, Inc., 342 F.3d 714, 722 (7th Cir. 2003) (quoting ILG Indus., Inc. v. Scott, 273 N.E.2d 393, 396 (Ill. 1971) ("An exact definition of a trade secret, applicable to all situations, is not possible. Some factors to be considered in determining whether given information is one's trade secret are [the six factors enumerated in the Restatement]." (internal quotation marks omitted)).

> encompassed [] above, *in which money damages are sought against a foreign state for* personal *injury* or death, or *damage to or loss of property, occurring in the United States and caused by the tortious act or omission of that foreign state or of any official or employee of that foreign state while acting within the scope of his office or employment*; except this paragraph shall not apply to—
>
> (A) *any claim based upon the exercise or performance or the failure to exercise or perform a discretionary function regardless of whether the discretion be abused*, or
>
> (B) any claim arising out of malicious prosecution, abuse of process, libel, slander, misrepresentation, deceit, or interference with contract rights.[131]

However, the FSIA Congressional report states that the Non-Commercial Tort Exception was enacted "to permit the victim of a traffic accident or other noncommercial tort to maintain an action against the foreign state . . . ."[132] Most courts have interpreted the Non-Commercial Tort Exception to require that the "entire tort" occurred in the U.S.[133] For example, the court in *Democratic National Committee v. Russian Federation et al.* held that the Non-Commercial Tort Exception did not apply to a cyberattack, which resulted in stolen sensitive information allegedly carried out by hackers who were located in Russia at the time of the hacking and who were working for the Russian government.[134] In so doing, the court stated, "the DNC's claims against the Russian federation are barred by the FSIA and no exception applies. Relief from the alleged activities of the Russian Federation should be sought from the political branches of the Government and not from the courts."[135] Accordingly, a suit against China for hacking and resulting misappropriation of trade secrets would likely not meet the requirements of the Non-Commercial Tort Exception.

D. SUMMARY OF EXISTING LEGAL REALITY

In general, existing state and federal laws provide U.S. companies with protections for their trade secrets and remedies when trade secret theft has occurred. This existing framework is nonetheless ill-suited to remedy Chinese trade secret theft because of standing, personal jurisdiction, immunity defense, and remedy limitations. A comprehensive strategy is

---

[131] 28 U.S.C. § 1605(a)(5) (emphasis added).

[132] Judi L. Abott, *The Noncommercial Torts Exception to the Foreign Sovereign Immunities Act*, 9 FORDHAM INT'L L.J. 134, 144 (1985) (quoting H.R. REP. NO. 1487, 94th Cong., 2d Sess., *reprinted in* 1976 U.S. CODE CONG. & ADMIN. NEWS 6604, 6619–20).

[133] Sam Kleiner & Lee Wolosky, *Time for a Cyber-Attack Exception to the Foreign Sovereign Immunities Act*, JUST SECURITY 2 (Aug. 14, 2019), https://www.justsecurity.org/65809/time-for-a-cyber-attack-exception-to-the-foreign-sovereign-immunities-act/.

[134] Democratic Nat'l Comm. v. Russian Fed'n, 392 F. Supp. 3d 410, 428 (S.D.N.Y. 2019) (relying on Doe v. Fed. Democratic Republic of Ethiopia, 851 F.3d 7 (D.C. Cir. 2017); Broidy Capital Mgmt., LLC v. Qatar, No. CV 18-2421-JFW(EX), 2018 WL 6074570, at *1 (C.D. Cal. Aug. 8, 2018)).

[135] *Democratic Nat'l Comm.*, 392 F. Supp. 3d at 429.

needed to extend existing trade secret protections extraterritorially, circumscribe or eliminate immunity defenses, and provide for effective remedies that compensate for and deter future misappropriation.

E. FEDERAL GOVERNMENT PURSUIT OF CLAIMS ASSIGNED BY U.S. COMPANIES IS NOT SUFFICIENT TO DETER CHINESE CYBERATTACKS

As an element of the NTSPS, the U.S. should adopt legislation that facilitates claims by private companies in U.S. courts and incentivizes private companies to pursue the claims or assign the claims to the federal government, notwithstanding the disincentives mentioned above and discussed in Section V. Providing extraterritorial jurisdiction and enforceable, meaningful pre-trial and post-judgment remedies will increase legal incentives to pursue claims, but the unmitigated economic pressures discussed in Section IV(F) may still deter private companies from pursuing claims directly or through assignment to the U.S. government.

Because private companies may decide not to pursue or assign claims, government enforcement of private claims for theft of National Security Information is unlikely to be effective in deterring and remedying theft of the same. To overcome these obstacles, the NTSPS proposes to position the U.S. federal government as the preferred plaintiff to deter and pursue theft of National Security Information by China and other international actors.

V. THE NATIONAL TRADE SECRET PROTECTION STRATEGY—A POLICY PRESCRIPTION TO SAFEGUARD U.S. NATIONAL SECURITY AND U.S. COMPANIES FROM CHINESE MISAPPROPRIATION

The proposed legislation takes the form of an authorizing amendment to the Defense Production Act of 1950,[136] the Homeland Security Act, or an entirely new legislative act, with corresponding regulatory amendments to the Defense Federal Acquisition Regulation Supplement ("DFARS"),[137] International Traffic in Arms Regulations ("ITAR"),[138] and other applicable sets of regulations. The legislation will (1) broadly define existing and future National Security Information as protected trade secrets in a comprehensive definition; (2) create a limited property right for the U.S. government in all of the protected information to create justiciability; (3) expressly extend existing and future federal protections for trade secrets to all protected information; (4) expressly provide that jurisdiction for U.S. federal courts to enforce such protections extends extraterritorially worldwide; (5) eliminate sovereign immunity in cases involving protected information; (6) subject all holders of U.S. debt instruments to the jurisdiction of U.S. federal courts; and (7) provide pre- and post-judgment

[136] Defense Production Act of 1950, 50 U.S.C. §§ 4501–4568 (2018).

[137] *See generally* 48 C.F.R. §§ 201.101–201.670 (2020); *Defense Federal Acquisition Regulation Supplement*, ACQUISITIONS.GOV, https://www.acquisition.gov/dfars (last visited July 29, 2020).

[138] *See generally* 22 C.F.R. §§ 120–130 (2020); *The International Traffic in Arms Regulations (ITAR)*, U.S. DEP'T OF ST.: DIRECTORATE OF DEF. TRADE CONTROLS, https://www.pmddtc.state.gov/?id=ddtc_kb_article_page&sys_id=24d528fddbfc930044f9ff621f961987 (last visited July 31, 2020).

remedies allowing U.S. companies and the U.S. government to satisfy amounts due by execution against U.S. government debt instruments held by China. The Congressional record and resulting NTSPS legislation should express clear intent for swift, aggressive, and thorough enforcement of the government's property right to ensure and promote U.S. national security.

A. A BROAD DEFINITION OF NATIONAL SECURITY TRADE SECRETS

This Article has, to this point, relied on existing law with respect to the definition and scope of National Security Information provided at the outset. That law is broad but not clearly inclusive of all types and qualities of information that may affect national security. A foundational element of the NTSPS is the adoption of legislation that broadly defines the information to be protected under the NTSPS as "National Security Trade Secrets." The definition should include all information presently included in National Security Information,[139] as well as all manners in which information is stored or maintained (e.g., paper, electronic, embodiment in a device, human memory, etc.) and, within electronic information, all means of storage, access, and use (e.g., memory drives in computers regardless of type, data servers, tablets, notebooks, and smart phones; flash or USB drives; disk drives; cloud storage; etc.). The NTSPS should express clear intent that the new, broad definition be applicable in cases and controversies brought under, among other things, the Economic Espionage Act of 1996,[140] Defend Trade Secrets Act of 2016,[141] Computer Fraud and Abuse Act,[142] and The National Stolen Property Act;[143] amendments to such legislation; and to all future legislation to protect National Security Trade Secrets.

B. A NEW, LIMITED GOVERNMENT PROPERTY RIGHT THAT ALLOWS THE U.S. GOVERNMENT TO PURSUE DIRECT CLAIMS

A necessary component of a party's ability to bring a lawsuit against another party is justiciability—whether there is a "case or controversy" between the parties within the meaning of Article III of the U.S. Constitution.[144] To have Article III standing, a plaintiff must have "'alleged such a personal stake in the outcome of the controversy' as to warrant invocation of federal-court jurisdiction and to justify exercise of the court's remedial powers on [its] behalf."[145] To meet the requirement of a personal stake in the litigation, a plaintiff must show the following: (1) the plaintiff has sustained "injury in fact" that is (a) "concrete and particularized" and (b) "actual or imminent";[146] (2) the complained-of injury was caused by the

[139] *See* Exec. Order No. 13,526, *supra* note 2 and corresponding text.
[140] 18 U.S.C. §§ 1831–39 (2018).
[141] *Id.* § 1836.
[142] *Id.* § 1030.
[143] *Id.* § 2314.
[144] Warth v. Seldin, 422 U.S. 490, 498 (1975).
[145] *Id.* (quoting Baker v. Carr, 369 U.S. 186, 204 (1962)).
[146] Lujan v. Defenders of Wildlife, 504 U.S. 555, 560 (1992) (internal quotation marks omitted).

defendants' action(s) or omission(s);[147] and (3) a resolution of the case favorable to the plaintiff is likely to redress the complained-of injury.[148]

Many cyberattacks to misappropriate National Security Information involve information owned by private companies. Private plaintiffs suffering trade secret misappropriation and the U.S. taking assignments of private claims will have standing under the principles discussed above. The U.S., however, does not have a clear property right in all National Security Information. This may prevent the U.S. from having justiciability in many circumstances.

To ensure standing, the U.S. should adopt legislation that facilitates direct government claims by providing the U.S. with a limited property right in all confidential National Security Information for the sole purpose of enforcing rights in such information.[149] To ensure the creation of this property right, the NTSPS legislation will require all future government contracts for goods or services derived from, containing, or potentially revealing any National Security Information to include the grant of a limited property right to the U.S. federal government, with the sole purpose and use to enforce confidential information and trade secret rights related to that good, service, or information.

The NTSPS-created property right will provide standing for the U.S. federal government to sue China for misappropriation of trade secrets[150] and to pursue all remedies now available under law, as well as remedies enabled or created by the NTSPS to strengthen the deterrent and compensatory effects of such remedies.

C. EXTRATERRITORIAL APPLICATION OF PROTECTIONS FOR NATIONAL SECURITY TRADE SECRETS

Courts are tasked with interpreting statutes to determine their meaning as understood by the legislative body that voted the bill in question into law.[151] "The most reliable evidence of that meaning is the text of the act itself."[152] Accordingly, Congress should take great care in crafting the NTSPS's enacting legislation so as to evidence Congress' intent to extend personal and subject matter jurisdiction extraterritorially for National Security Trade Secrets. Stating as much in an explicit manner, where the

---

[147] *Id.*

[148] *Id.* at 561.

[149] This limited national security property right would not diminish the economic property right held by the private company that developed the trade secret.

[150] While the NTSPS calls for the creation of a limited federal government property right related to all intellectual property developed in connection with existing government defense contracts, the litigation strategy only applies to trade secrets. Restricting the NTSPS' litigation strategy to just trade secret-related violations shines additional light on how the securing of trade secrets through cyber hacking or other similar techniques is an objectively nefarious act. For while different countries may have significantly varying views on the property rights associated with the publicly available classes of intellectual property (e.g., patents, copyrighted works, trademarks), the very term "trade secret" indicates that the property right involves confidential information not available from or to public sources.

[151] Overseas Educ. Ass'n, Inc. v. Fed. Labor Relations Auth., 876 F.2d 960, 974 (D.C. Cir. 1989).

[152] *Id.*; *see also* United States v. Ron Pair Enters., Inc., 489 U.S. 235, 241 (1989) ("[W]here . . . the statute's language is plain, 'the sole function of the courts is to enforce it according to its terms.'" (citation omitted)).

legislature's intent is clear on the face of the law, should foreclose unnecessary, extensive inquiry into legislative history.[153]

D. WITHDRAWAL OF SOVEREIGN IMMUNITY PROTECTIONS IN CASES ALLEGING THEFT OF NATIONAL SECURITY TRADE SECRETS

As discussed hereinabove, U.S. companies and/or the U.S. government may be able to utilize several of the exceptions to the FSIA to pursue trade secret misappropriation suits against China and other international cybercriminals. Nonetheless, the FSIA remains a formidable obstacle for plaintiffs seeking to sue foreign sovereigns in U.S. courts. Given the serious national security and economic implications of China's rampant cyberattacks and related trade secret misappropriation in the U.S., Congress would be more than justified in carving out a specific exception to sovereign immunity protections in cases alleging theft of national security trade secrets. This could be accomplished through an amendment to the FSIA, which explicitly states the exception's deterrent and remedial purposes.

E. SUBJECTING HOLDERS OF U.S. DEBT INSTRUMENTS TO JURISDICTION OF U.S. FEDERAL COURTS

Enforcement of the NTSPS requires that U.S. federal courts have personal and subject matter jurisdiction over misappropriators. To simplify these analyses, the NTSPS calls for U.S. debt instruments to contain language that the debt holder consents to personal jurisdiction of the federal courts in the judicial district in which the private plaintiff is formed, is organized, or maintains its principal place of business,[154] or in which the U.S. government, as the plaintiff, maintains a U.S. Attorney's Office. Such jurisdiction will force China and its surrogates to defend claims of misappropriation and thereby account for their conduct or allow the claims to be proven up after default. In either case, under the NTSPS, a successful plaintiff will then have a right to satisfy its judgment from a more readily available asset class than now exists under federal law.

F. CREATION OF FEDERAL RIGHTS THROUGH EXISTING FEDERAL TRADE SECRET LAWS TO ATTACH AND LIEN U.S.-ISSUED DEBT INSTRUMENTS PRE-TRIAL AND EXECUTE ON THE SAME POST-JUDGMENT

In addition to existing remedies, the NTSPS will provide private parties and the U.S. with an expedited procedure to obtain prejudgment remedies. Specifically, it will provide that U.S. Treasury securities and other U.S. debt obligations held by, or in the name of, a foreign nation or private

[153] *Id.* (quoting Burlington N. R.R. Co. v. Okla. Tax Comm'n, 481 U.S. 454, 461 (1987) ("As the Supreme Court has recently emphasized, a judicial determination that statutory language is clear ordinarily forecloses further inquiry into legislative intent: 'Unless exceptional circumstances dictate otherwise, [w]hen we find the terms of a statute unambiguous, judicial inquiry is complete.'" (citation omitted))).

[154] This could be accomplished by amending 28 U.S.C. § 1391 to include plaintiff-specific venue provisions.

entity/person may be attached, or a lien placed upon them, pending trial and are subject to execution after judgment.

For private plaintiffs, the NTSPS will restate the applicability of Federal Rule of Civil Procedure 64, which provides that U.S. district courts may use either federal procedures for prejudgment remedies or those provided by the state in which the district court sits.[155]

For the government, the Federal Debt Collection Procedures Act of 1990[156] will be amended to expressly include all forms of U.S. government debt held by foreign sovereigns.[157] The definition of "Property" in the Act will include express reference to National Security Trade Secrets and their definition. The NTSPS will further amend the Federal Debt Collection Procedures Act of 1990 to work in connection with Rule 64 of the Federal Rules of Civil Procedure to enable private parties and the U.S. filing any action based on trade secret misappropriation to obtain attachment, injunction, garnishment, replevin, sequestration, and other corresponding or equivalent remedies. Notably, the U.S. already has laws on the books that allow for comparable "administrative offsets" where the U.S. owes monies.

The enabling legislation will also include an expedited time frame for hearing on the sought-after remedies, make the remedies available in all cases of alleged theft of National Security Trade Secrets, allow courts to rely on credible hearsay in determining the probable validity of a claim, create a presumption of irreparable harm, and eliminate bond requirements.

G. UTILIZATION OF EXISTING PROCEDURES TO PROTECT NATIONAL SECURITY INFORMATION TRADE SECRETS AND U.S. CYBER CAPABILITIES DURING DISCOVERY

The U.S. legal system has procedures to protect highly sensitive information during litigation. The two existing tools most likely to be helpful are protective orders and filing documents under seal. Protective orders, which are granted in federal courts pursuant to Rule 26 of the Federal Rules of Civil Procedure, are used to protect a party's confidential information from being disclosed to the general public.[158] Specifically, Rule 26(c)(1)(G) provides the Court may "protect a party or person from annoyance, embarrassment, oppression, or undue burden or expense, including . . . requiring that a trade secret or other confidential research,

[155] Rosen v. Cascade Int'l, Inc., 21 F.3d 1520, 1530–31 (11th Cir. 1994) (quoting FED. R. CIV. P. 64) ("Rule 64 makes available to district courts 'all remedies providing for seizure of person or property for the purpose of securing satisfaction of the judgment ultimately to be entered in the action' and provides that, except as otherwise provided by the Constitution or an applicable federal statute, such remedies 'are available under the circumstances and in the manner provided by the law of the state in which the district court is held.' The rule expressly lists attachment as one such available remedy, along with 'other corresponding or equivalent remedies, however designated.' As the Supreme Court has explained, 'long-settled federal law provid[es] that in all cases in federal court, . . . state law is incorporated to determine the availability of prejudgment remedies for the seizure of person or property to secure satisfaction of the judgment ultimately entered.' Granny Goose Foods, Inc. v. Brotherhood of Teamsters Local 70, 415 U.S. 423, 436 n.10 (1974).").

[156] 28 U.S.C. §§ 3001–3308 (2018).

[157] *Id.* § 3002(12).

[158] Phillips ex rel. Estates of Byrd v. Gen. Motors Corp., 307 F.3d 1206, 1210–11 (9th Cir. 2002).

development, or commercial information not be revealed or be revealed only a specified way" if "good cause" is shown.[159]

However, a protective order by itself is not necessarily sufficient to protect the confidentiality of the documents it protects. As the U.S. Court of Appeals for the Third Circuit explained in *Pansy v. Borough of Stroudsburg*, "[W]hen a court enters an order of protection over documents exchanged during discovery, and these documents have not been filed with the court, such documents are not, by reason of the protective order alone, deemed judicial records to which the right of access attaches."[160]

A party seeking to seal documents must overcome the general rule that the public has a right to access information from judicial proceedings, including court records.[161] To do this, the moving party must meet one of two standards: (1) the compelling reasons standard, or (2) the good cause standard.[162] As the good cause standard usually applies to "sealed materials attached to a discovery motion unrelated to the merits of a case,"[163] it is unlikely to apply in cases that arise under the NTSPS and therefore is not discussed in detail here.

The compelling reasons test, which is likely to apply to cases arising under the NTSPS, requires that a party moving to seal a record must demonstrate "compelling reasons" that are supported by specific factual findings.[164] "What constitutes a 'compelling reason' is 'best left to the sound discretion of the trial court.'"[165] Courts have previously found that "sources of business information that might harm a litigant's competitive standing" can be a sufficient compelling reason.[166] Likewise, courts have found that information that poses "[n]ational security concerns can, of course, provide a compelling reason for shrouding in secrecy even documents once in the public domain."[167] If the moving party can show it has "compelling reasons" to seal the document, these reasons will be balanced against the public's interest in disclosure.[168] The NTSPS will

---

[159] FED. R. CIV. P. 26(c)(1).

[160] Pansy v. Borough of Stroudsburg, 23 F.3d 772, 782 (3d Cir. 1994) (citing Seattle Times Co. v. Rhinehart, 467 U.S. 20, 30–37 (1984); Leucadia, Inc. v. Applied Extrusion Techs., Inc., 998 F.2d 157, 163 & n.9 (3d Cir. 1993); Cipollone v. Liggett Group, Inc., 785 F.2d 1108, 1119–20 (3d Cir. 1986), *cert. denied*, 484 U.S. 976 (1987)).

[161] "Historically, courts have recognized a 'general right to inspect and copy public records and documents, including judicial records and documents.'" Kamakana v. City & Cty. of Honolulu, 447 F.3d 1172, 1178 (9th Cir. 2006) (internal quotation marks and citation omitted) (quoting Nixon v. Warner Commc'ns, Inc., 435 U.S. 589, 597 & n.7 (1978)). "The presumption of access is 'based on the need for federal courts, although independent—indeed, particularly because they are independent—to have a measure of accountability and for the public to have confidence in the administration of justice.'" Ctr. for Auto Safety v. Chrysler Grp., LLC, 809 F.3d 1092, 1096 (9th Cir. 2016) (quoting United States v. Amodeo (Amodeo II), 71 F.3d 1044, 1048 (2d Cir. 1995)).

[162] *Ctr. for Auto Safety*, 809 F.3d at 1096–97.

[163] *Id.* at 1097.

[164] *Id.* ("[A] court may seal records only when it finds 'a compelling reason and articulate[s] the factual basis for its ruling, without relying on hypothesis or conjecture.'" (quoting *Kamakana*, 447 F.3d at 1179)).

[165] *Id.* at 1097 (quoting Nixon, 435 U.S. at 599).

[166] *Id.*

[167] Ground Zero Ctr. for Non-Violent Action v. U.S. Dep't of Navy, 860 F.3d 1244, 1262 (9th Cir. 2017) (citing Al-Haramain Islamic Found., Inc. v. Bush, 507 F.3d 1190, 1193 (9th Cir. 2007) (permitting the government to seal a Top Secret classified document pursuant to the common law state secrets privilege, despite its prior dissemination to the public)).

[168] *Ctr. for Auto Safety*, 809 F.3d at 1096.

provide that National Security Trade Secrets, including the cyber capabilities of the U.S. government and its military contractors, are presumed to satisfy this test.

H. SUMMARY OF AMENDMENTS TO EXISTING LEGISLATION TO INCLUDE PROTECTION OF NATIONAL SECURITY TRADE SECRETS

To effectively accomplish the foregoing aspects of the NTSPS, Congress must pass amendments to, among other things, the Economic Espionage Act of 1996, Defend Trade Secrets Act of 2016, Computer Fraud and Abuse Act, and The National Stolen Property Act to expressly (1) incorporate the broad definition of National Security Trade Secrets; (2) affirm the U.S. government as an owner of National Security Trade Secrets in all circumstances with the right to enforce the provisions of each act; and (3) state Congressional intent to extend each act extraterritorially in cases involving National Security Trade Secrets, regardless of whether the plaintiff is the U.S. government or a private individual or entity. Additionally, the NTSPS will include amendments to the FSIA to eliminate all sovereign immunity defenses in cases involving National Security Trade Secrets upon the determination by the Executive Branch or its delegate that proceeding with the claim is consistent with U.S. foreign policy. Finally, the NTSPS will include a new act under U.S.C. Title 28 empowering U.S. federal courts to provide for and facilitate the prejudgment attachment of U.S. debt instruments and post-judgment execution on such instruments.

In sum, the NTSPS aligns the incentive structure to provide the U.S. government with clear standing to pursue direct claims for misappropriation of any and all National Security Trade Secrets trade against China and other international actors under existing, applicable federal law. While implementation of the NTSPS would allow the U.S. government to achieve a litany of important policy goals, it may also give rise to unintended national security, geopolitical, and economic ramifications. These potential ramifications are discussed hereinbelow.

VI. POTENTIAL NATIONAL SECURITY AND GEOPOLITICAL RAMIFICATIONS AND REASONS WHY THE U.S. GOVERNMENT AND U.S. COMPANIES MAY NOT WANT TO UTILIZE THE PROPOSED NTSPS

Despite the fraying relationship between China and the U.S., the two countries' economies are intertwined. Americans rely heavily on Chinese-made products, many Americans work for Chinese-owned companies, and China remains an important lender to the U.S. government and is one of its most important trading partners.[169] Heightening the potential impact of the NTSPS is the projection that China will overtake the U.S. in total economic output sometime in the next decade, thereby sharpening the competition with the two nations over markets, resources, technological advancement,

[169] Feffer, *supra* note 38.

and geopolitical advantage.[170] The recognition of these strong connections likely makes presidential administrations hesitant to implement policy prescriptions that might generate comparable, costly retaliations by China.

The NTSPS has numerous potential geopolitical ramifications, including (1) withdrawal of additional Chinese credit to the U.S. treasury; (2) withdrawal of public and private investments from U.S. markets; (3) seizure of U.S. individual, government, and company assets located in China; (4) U.S. companies being forced out of Chinese markets; (5) and comparable suits by the Chinese government against the U.S. for U.S. cyber espionage. Each of these is briefly discussed below.

A. WITHDRAWAL OF CHINESE GOVERNMENT FINANCING FROM THE U.S. TREASURY

Policy commentators have noted that the U.S.'s "continued dependence on foreign borrowing is a significant vulnerability in the event of shock, such as a collapse in U.S. housing prices, or an extreme national security breach, that might slow the inflow of new funds into the United States."[171] However, should China try to use its financial leverage to upset the U.S. economy, such action is likely to backfire. For example, if China were to suddenly convert a large share of its predominantly U.S. dollar portfolio into Euros, the resulting decline in the U.S. dollar would hurt both U.S. finances and the Central Bank of China in the form of significant capital losses.[172] As analysts at the Brookings Institution have noted, "Fundamentally, when a debtor owes the bank a large enough amount, the debt becomes the bank's problem. China, whose reserves amount to 50 percent of its GDP, faces risks far to[o] great to ever seriously consider [such a radical financial move against the U.S]."[173]

So not only is China's complete financial withdrawal from the U.S. Treasury market unlikely, but if China were to take such action, the U.S. has an unmatched ability to borrow money due to its sterling in debt markets.[174]

Policy analysts have echoed these sentiments, noting that the U.S. exposure in global debt markets poses a significantly greater risk in other scenarios than does China liquidating its financial leverage over the U.S. en masse. Notably, the U.S.'s account deficit "could significantly amplify the effects of growth crisis precipitated either by economic factors (say, a historic collapse in housing prices), or geopolitical factors (such as a terrorist attack of unprecedented dimensions on U.S. soil)."[175]

---

[170] *Id.*

[171] Kenneth Rogoff, *Foreign Holdings of U.S. Debt: Is Our Economy Vulnerable?*, BROOKINGS INST. (June 26, 2007), https://www.brookings.edu/testimonies/foreign-holdings-of-u-s-debt-is-our-economy-vulnerable/.

[172] In 2007, it was projected that a 20 percent drop in the dollar against the Yuan would cost the Chinese Central Bank well over a hundred billion dollars. *Id.*

[173] *Id.*

[174] Rachel Konig Beals, *Fitch Cuts U.S. Credit Outlook to 'Negative' on COVID-19, Election Uncertainty, but Maintains AAA Rating*, MARKETWATCH (July 31, 2020, 6:37 PM), https://www.marketwatch.com/story/fitch-cuts-us-credit-outlook-to-negative-on-covid-19-election-uncertainty-but-maintains-aaa-rating-2020-07-31.

[175] Rogoff, *supra* note 171.

Economic projections by the Brookings Institution indicate that if the U.S. "were forced to cut back the flow of its new borrowing by say, a half — to $400 billion per year, the trade-weighted dollar could easily fall 20-25 percent, and interest rates could rise by close to one percent across the board. On impact, it is quite possible that financial markets would overshoot."[176] China could undertake retaliatory action against the U.S. to prompt these negative market outcomes. Such economic conditions, should they come to fruition, would augment the severity and prolong the duration of a financial crisis.[177]

B. WITHDRAWAL OF CHINESE PRIVATE INVESTMENTS FROM U.S. MARKETS

U.S. financial services companies are arguably the country's most successful export.[178] Implementing the NTSPS may either drive foreign entities from engaging in the U.S. or lead to economic retribution that backfires and results in harm to U.S. interests, or both.

While many Chinese giants and start-ups alike have chosen to be listed on U.S.-based stock exchanges to receive a perceived boost to their brand and access to U.S. capital,[179] Chinese companies seem to be increasingly utilizing stock exchanges in other countries.[180] Additionally, it appears there is a growing concerted effort by the Chinese government to have Chinese-based companies list their stock on Chinese-based exchanges. For example, in July 2019, the Chinese government launched a new stock board, aimed at creating "a better environment for technology companies to go public."[181]

The impact of the withdrawal of Chinese capital and related investment opportunities may not facilitate as drastic a change as one might expect. There already exists federal limitations and oversight on Chinese investment in certain sectors. One such piece of legislation providing for this oversight and related limitations is the Foreign Investment Risk Review Modernization Act of 2018 ("FIRRMA"), which significantly augmented the ability of the Committee on Foreign Investment in the United States ("CFIUS") to conduct reviews on how, if at all, certain foreign investments in the U.S. could have national security implications.[182] Additional restrictions have been proposed and await final approval.[183]

---

[176] *Id.* (providing calibrations on how a closing up of the U.S. current account might affect the trade weighted U.S. exchange rate).

[177] *Id.*

[178] Rogoff, *supra* note 171.

[179] Evelyn Chang, *Constricting Investments Into Chinese Companies Could Hit the US as Hard as it Hits China*, CNBC (Sept. 30, 2019, 7:46 AM), https://www.cnbc.com/2019/09/30/pulling-out-us-investments-from-china-could-hurt-america-more-analysts.html. Notable Chinese companies that have chosen to focus on raising capital in the U.S. include technology giant Alibaba. *Id.*

[180] *Id.* Notably, technology company Tencent, food delivery company Meituan-Dianping, and smartphone maker Xiaomi all decided to go public in Hong Kong last year. *Id.*

[181] *Id.*

[182] John R. Ingrassia et al., *CFIUS Proposed Rules Target Critical Technology, Sensitive Personal Data and Real Estate*, MONDAQ (Oct. 18, 2019), http://www.mondaq.com/unitedstates/x/855212/Inward+Foreign+Investment/CFIUS+Proposed+Rules+Target+Critical+Technology+Sensitive+Personal+Data+And+Real+Estate.

[183] *Id.*

C. SANCTIONS AND SEIZURE OF U.S. INDIVIDUAL AND ENTITY ASSETS IN CHINA

Should the U.S. proceed with implementation of the NTSPS, China may blame a U.S. defense company implicated in related litigation for any resulting "damages"—whether in terms of a judgment and/or legal fees and costs incurred. In such a situation, China may decide to help offset Chinese damages by seizure of assets or retaliate by sanctioning the U.S. company's business (whether directly or via its buyers, suppliers, etc.). This is not a remote worry, as China has already shown its willingness to sanction U.S. defense companies involved in concerted U.S. action in other contexts that implicate sovereignty and national security concerns.[184]

D. U.S. COMPANIES BEING FORCED OUT OF CHINESE MARKETS

The legal actions proposed in this Article may lead to the Chinese government retaliating against U.S. companies by forcing them out of Chinese markets, which are growing in importance for American companies, including the likes of major defense contractors Honeywell,[185] Boeing,[186] Cummins,[187] and Parker Aerospace.[188] For example, China has been Honeywell's fastest growing market since 2005.[189] During roughly the same time period, Honeywell's China-based workforce nearly tripled and revenue attributable from the Chinese market increased sixfold to roughly $3 billion, making China Honeywell's largest market outside of the U.S.[190] Similarly, Cummins, which has many manufacturing plants in China, has noted that more than 1/3 of all engines sold last year were sold in China, with the resulting revenue crucial to helping pay for the company's research and development costs during downturns in the U.S. market.[191]

While China-related economic debates in the U.S. usually focus on the U.S. trade deficit[192] or the number of jobs lost in the U.S. as U.S.-based

---

[184] Chun Han Wong, *China Threatens to Sanction Lockheed Martin Over Taiwan Arms Deal*, WALL ST. J. (July 14, 2020, 12:55 PM), https://www.wsj.com/articles/china-to-sanction-lockheed-martin-over-taiwan-arms-deal-11594727908 (discussing China's threats to sanction Lockheed Martin for its part in a $620 million U.S. arms package for Taiwan—a self-ruled island democracy that China continues to assert is part of its territory).

[185] *U.S. Conglomerate Honeywell Sees Tremendous Opportunities in China*, CGTN (Sept. 25, 2019, 4:20 PM), https://news.cgtn.com/news/2019-09-25/U-S-conglomerate-Honeywell-sees-tremendous-opportunities-in-China-Kh9necm7zq/index.html (reporting Honeywell's massive growth of employee headcount, revenue, investment, and other metrics related to its China operations).

[186] Jim Zarolli, *U.S. Companies in China Get Caught in the Trade War Crossfire*, NPR (Aug. 27, 2019, 5:22 PM), https://www.npr.org/2019/08/27/754777224/u-s-companies-in-china-get-caught-in-the-trade-war-crossfire.

[187] *Id.*

[188] Courtney E. Howard, *Parker E. Aerospace and AVIC Form Two Joint Ventures in Support of New COMAC C919 Aircraft*, INTELLIGENT AEROSPACE (June 16, 2013), https://www.intelligent-aerospace.com/commercial/article/16539634/parker-aerospace-and-avic-form-two-joint-ventures-in-support-of-new-comac-c919-aircraft.

[189] *Id.*

[190] *Id.*

[191] Zarolli, *supra* note 186.

[192] David J. Lynch & Anna Fitfield, *Trump Delays Increase in Tariffs on Chinese Goods by Two Weeks 'As A Gesture of Good Will'*, WASH. POST (Sept. 11, 2019, 6:15 PM), https://www.washingtonpost.com/world/asia_pacific/china-to-remove-tariffs-on-some-us-products-but-not-pork-or-soybeans/2019/09/11/79d45fc0-d459-11e9-8924-1db7dac797fb_story.html ("Trump has

companies have shifted manufacturing efforts overseas,[193] what is often overlooked is the growing importance of China as a consumer market. As Shaun Rein, Managing Director of the China Market Research Group, has stated, "China has become the largest market to sell into for many of America's largest companies."[194]

Anna Ashton, Senior Director of Government Affairs at the U.S.-China Business Council, noted that the opportunities for U.S. companies to make money abound in China, and that "[t]he vast majority of [U.S.] companies have consistently reported and continue to report every year that their China operations are profitable—and not just profitable but more profitable than their operations overall."[195]

The growth of the Chinese market for U.S. companies shows few signs of slowing, as China's middle class is now more populous than the entirety of the U.S. population, and some analysts believe this large group will lead China and the rest of the world to new levels of prosperity.[196] Starbucks CEO Kevin Johnson sees significant long-term growth, noting, "[t]he market in China — I am so bullish on it for the long term . . . . We're going to be able to accelerate and build new stores for a long, long time in China."[197]

The profitability and growth of U.S. companies in China might be at risk if the solution proposed herein is implemented. China has shown that it is willing and able to retaliate on both a geopolitical[198] and individual-company level.[199] For example, after Marriott Hotels referred to Taiwan as a country separate from China, the Chinese government shut down Marriott's online reservation system for a week.[200]

If China decided to retaliate against the U.S.—either directly or by hurting U.S. companies—it could cause great financial harm to U.S.

---

been particularly concerned about the trade deficit with China — which widened to $419 billion last year — and has been pressing Beijing to buy more from the United States as a way to close that gap.").

[193] Jeffrey Bartash, *China Really is to Blame for Millions of Lost U.S. Manufacturing Jobs, New Study Finds*, MARKETWATCH (May 14, 2018, 1:30 PM), https://www.marketwatch.com/story/china-really-is-to-blame-for-millions-of-lost-us-manufacturing-jobs-new-study-finds-2018-05-14 (citing David Autor et al., *Competition from China Reduced Innovation in the US*, VOX (Mar. 20, 2017), https://voxeu.org/article/competition-china-reduced-innovation-us) ("Low Chinese wages and a cheap Chinese currency — at a time when the dollar was strong — gave China several huge advantages. Companies shuttered operations in the U.S., moved to China and eventually set up research hubs overseas in another blow to the America's economic leadership."). *But see* Chen Gong, *What Makes China's Latest Wave of Foreign Capital Withdrawal Different? It's Structural*, S. CHINA MORNING POST (July 29, 2019, 3:00 AM), https://www.scmp.com/comment/opinion/article/3020234/what-makes-chinas-latest-wave-foreign-capital-withdrawal-different (noting that a large number of non-China-based companies, including large U.S. companies such as Walmart, are selling significant stakes in their Chinese operations and/or removing their manufacturing operations from China. Specifically, the report notes, "The scale of foreign investment in high-end manufacturing is shrinking fast, according to our analysis, and there is almost no new investment in some Shanghai industrial parks.").

[194] Zarolli, *supra* note 186.

[195] *Id.*

[196] *Id*. However, not all analysts are as optimistic about the Chinese middle class's impact on the Chinese and global economy. Some question the true size and relative wealth of the class and express skepticism about the group's continued viability moving forward in the face of high costs, rising debt, and weak income growth. *Id.*

[197] *Id.*

[198] *See, e.g.*, Daniel Shane, *China Hits the United States with Tariffs on $3 Billion of Exports*, CNN: BUSINESS (Apr. 2, 2018, 9:59 AM), https://money.cnn.com/2018/04/02/news/economy/china-us-tariffs-trade/index.html.

[199] *See, e.g.*, Zarolli, *supra* note 186.

[200] *Id.*

interests. Examples of actions that the Chinese could easily take include imposing heavy fines for business infractions; restricting work visas; and slowing down or altogether frustrating the permitting processes required for the creation of new stores, plants, and other buildings. In terms of indirectly impacting the U.S. economy, the Chinese government could encourage its people to boycott some or all U.S. companies.

China has already taken comparable actions against other countries in the past. For example, in response to South Korea's installation of a U.S.-developed anti-missile system, China ordered its travel agencies not to send Chinese tour groups to South Korea, thereby significantly hurting South Korea's tourism industry.

While China has not yet taken such actions against American companies, this does not mean that China is not able or willing to do so.[201] Should the above-proposed solution be effectuated, the Chinese government may have no choice, if for no other reason than to try to save face, than to take aim at U.S. businesses and their interests in China. Such retaliation would hurt the stock prices of U.S. companies, which would likely have additional negative political and economic externalities.

E. U.S. INVESTORS HAVING NO ACCESS, OR LIMITED ACCESS, TO CHINESE-ORIGINATING INVESTMENT VEHICLES

Analysts believe that Chinese stocks constitute a significant investment opportunity with a high likelihood for long-term growth.[202] While U.S. investment in Chinese-based stocks remains limited, the Chinese government is working to open up its markets to foreign investors—specifically institutional investors, many of which are based in the U.S.[203] Conversely, Chinese stocks are gaining more traction on global indexes.[204] The global stock index provider MSCI has added many Chinese A-Share stocks to its emerging markets index in recent years, and in early 2019 Bloomberg Barclay Global Aggregate Index and J.P. Morgan's benchmark bond index both started to include Chinese bonds and debt.[205] Additional integration of Chinese assets in U.S.-based stock and bond indexes, or global indexes in which U.S. companies and citizens have high exposure, could mean that Americans are indirect investors in China's capital markets through one of a host of investment vehicles.[206] Should the Chinese restrict U.S. involvement in such investments, Americans may lose out on what is expected to be a very profitable long-term investment story.[207]

[201] *Id.*
[202] Chang, *supra* note 179.
[203] *Id.*
[204] *Id.*
[205] *Id.*
[206] *Id.*
[207] *Id.*

F. COMPARABLE SUITS BY THE CHINESE AGAINST THE U.S. IN CHINESE COURTS

Chinese-American frustration over cyberattacks is not a one-way street, with China-based companies allegedly being the subject of U.S. government-backed cyberattacks.[208] For example, in September 2019, technology giant Huawei accused the U.S. government of hacking the company's internal information systems in an effort to disrupt the company's business operations.[209] Claims brought by the U.S. government or U.S. private companies against China for theft of National Security Trade Secrets could trigger retaliatory claims either as defensive moves or because there are justiciable issues arising from U.S. counter-espionage activities. Such claims will likely implicate national security concerns, hence the need for Executive Branch/State Department review of claims prior to filing as discussed above. Retaliation between the two countries has become increasingly public in recent years, with President Trump's administration publicly stating its intent to carrying out counter-cyberattacks against China for continued and worsening theft of U.S. technology.[210]

G. U.S. COMPANIES AND THE U.S. GOVERNMENT MAY HAVE CONCERNS ABOUT MAKING THEIR CYBERSECURITY VULNERABILITIES, PROTOCOLS, AND TECHNIQUES PART OF THE COURT'S RECORDS

Success in prosecuting the cases of the type contemplated by the NTSPS will require (1) proof that a cyberattack occurred; (2) that the misappropriated information constitutes National Security Trade Secrets; and (3) that the cyberattack was carried out, or at least facilitated, approved or sanctioned by, the Chinese government. This would likely be an evidence-intensive process that may reveal the National Security Trade Secrets in discovery, at hearings, and at trial. Disclosure of the information, even if subject to protective orders and through a sealing process as discussed in Section IV(G), may seriously compromise the National Security Information, and may also reveal U.S. cyber-capabilities.

While these protective tools, if they are utilized to their most restrictive extent, limit the public's access to sensitive documents, they would not keep Chinese litigation teams—including lawyers, staff, and expert witnesses—from viewing the documents and learning their content. These individuals, if technically knowledgeable about cybersecurity, could gain an intimate understanding of the sensitive infrastructure information and report back to pertinent parties in the Chinese government cyber community. U.S. companies and the U.S. government may be understandably reluctant to pursue litigation because they may perceive these risks to be greater than the benefits of pursuing claims.

---

[208] *See, e.g.*, Aimee Picchi, *Huawei Claims U.S. Threatened Employees and Attacked its Network*, CBS NEWS (Sept. 3, 2019, 1:02 PM), https://www.cbsnews.com/news/huawei-p30-phone-maker-claims-u-s-is-menacing-its-employees-and-attacking-its-network/.

[209] *Id.*

[210] Bill Gertz, *Inside the Ring: U.S. Hits Back Against Chinese Cyberattacks*, WASH. TIMES (Mar. 6, 2019), https://www.washingtontimes.com/news/2019/mar/6/us-counters-china-cyberattacks/.

H. U.S. COMPANIES LIKELY UNDERREPORT CYBERSECURITY BREACHES AND WOULD NOT WANT TO SELF-IMPOSE MORE STRINGENT COMPLIANCE COSTS

Many U.S. states have privacy protection laws that require businesses to notify consumers of any breach of security where a hacker gains access to the business's customers' sensitive information (e.g., confidential or otherwise personally identifying).[211] Additionally, depending on the type of information that was subject to the breach, the target company may have a host of additional federal reporting requirements.[212] Companies' non-compliance with such laws have led to significant financial penalties.[213] For example, in 2018, Uber was fined $148 million for violation of state data breach notification laws in relation to a 2016 breach of over 57.5 million driver and user accounts.[214]

Despite costly fines for not reporting cyber breaches, or not doing so in an expeditious manner, it is likely that U.S. companies still significantly underreport the rate of cyber breaches they suffer. For example, the unit chief of the Federal Bureau of Investigation's Internet Crime Complaint Center has said that the aggregate number of cyber-crimes reported yearly only represents 10–12 percent of the actual number of crimes committed.[215] If U.S. companies do not report when they have suffered a cyberattack, then the DOJ and similar prosecutorial agencies cannot pursue claims against the Chinese government. Underreporting, and therefore under-filing of cyberattack-related litigation, may decrease the effectiveness of the deterrence role hoped for as part of the strategy proposed in this Article. However, at least in the context of U.S. defense companies, underreporting should not be a significant issue after the enactment of the Defense Federal Acquisition Regulation Supplement 252.204-7012, titled "Safeguarding

---

[211] FED. TRADE COMM'N, DATA BREACH RESPONSE: A GUIDE FOR BUSINESS 4 (May 2019).

[212] *See, e.g.*, *id.* at 1, 5 (If the breach involved electronic health information, the attacked company may need to abide by the Health Breach Notification Rule ("HBNR") and/or the HIPPA Breach Notification Rule. Complying with the HBNR requires the affected company to notify the FTC of the breach, and in certain cases, also the media); *CF Disclosure Guidance: Topic No. 2 Cybersecurity*, DIVISION OF CORP. FIN.: SEC. & EXCHANGE COMMISSION (Oct. 13, 2011), https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm (SEC disclosure rule requiring that publicly traded companies who are compromised by a cyberattack disclose said cyberattack to regulators and explain the measures the company plans to take to close their cyber-security gaps); FIN. CRIMES ENF'T NETWORK, U.S. DEP'T OF THE TREASURY, FIN-2016-A005, ADVISORY TO FINANCIAL INSTITUTIONS ON CYBER-EVENTS AND CYBER-ENABLED CRIME 4 (2016), https://www.fincen.gov/sites/default/files/advisory/2016-10-25/Cyber%20Threats%20Advisory%20-%20FINAL%20508 2.pdf (FinCEN advisory outlining the reporting requirements for financial institutions that suffer a cyber breach).

[213] Dan Swinshoe, *The Biggest Data Breach Fines, Penalties and Settlements So Far*, CSO (July 26, 2019, 3:00 AM), https://www.csoonline.com/article/3410278/the-biggest-data-breach-fines-penalties-and-settlements-so-far.html.

[214] Kate Conger, *Uber Settles Data Breach Investigation for $148 Million*, N.Y. TIMES (Sept. 26, 2018), https://www.nytimes.com/2018/09/26/technology/uber-data-breach.html.

[215] Matt Powell, *11 Eye Opening Cyber Security Statistics for 2019*, CPO MAG. (June 25, 2019), https://www.cpomagazine.com/cyber-security/11-eye-opening-cyber-security-statistics-for-2019/; *see also* Jim Brashear, *Senators Ask SEC for Guidance on Information Security Risk Disclosure*, THECORPORATECOUNSEL.NET (June 9, 2011), https://www.thecorporatecounsel.net/blog/2011/06/senators-ask-sec-for-guidance-on-information-security-risk-disclosure.html (reporting that a 2009 survey conducted by insurance underwriter Hiscox Ltd. found that 38 percent of Fortune 500 companies made a "significant oversight" by failing to mention privacy or data security exposures in their public disclosures).

Covered Defense Information and Cyber Incident Report."[216] This regulation imposes a mandatory reporting obligation that requires, among other things, (1) furnishment of a cyber incident report to the Defense Department within 72 hours of the incident's discovery; (2) production of the malicious software used to the Defense Department, if possible; (3) cooperation with the Defense Department if it decides to undertake a forensic investigation; and (4) the notification of parties downstream in the supply chain of the breach.[217]

I. SUMMARY OF IMPEDIMENTS TO USAGE OF THE NTSPS

As referenced at the outset, Chinese cyberattacks are a pernicious problem that persists notwithstanding the damages they cause to national security and U.S. economic interests. Efforts to combat the cyberattacks at an economic level have been unsuccessful to date in part because of the impediments discussed above. The NTSPS is intended to overcome the impediments by providing a clearer and more direct path to obtaining an economic remedy for those damaged by cyber-espionage.

CONCLUSION

For the most part, the current geopolitical relationship between the U.S. and China can be characterized as a tense truce between political rivals who, for the time being and not withstanding public posturing, need one another to move their economic agendas forward. With China quickly closing the economic and geopolitical influence gaps between itself and the U.S., a significant restructuring of the relationship is likely and will not be easy or painless. The U.S. should be proactive in protecting its economic and national security interests by implementing the course of action proposed in this Article and incorporating the NTSPS into U.S. foreign and defense policies. Doing so will (1) compensate the U.S. for damages resulting from Chinese-led or -sponsored cyberattacks; (2) deter future Chinese cyberattacks by conveying a strong message that the U.S. will take strong and meaningful action in response to said attacks; (3) slow the advancement of Chinese military and national security technology by forcing China to internalize the significant research and development expenses incurred by the U.S. to develop the technological capabilities often targeted by cyber espionage initiatives; (4) significantly reduce U.S. debt and the weight it places on the U.S. economy and foreign policy; and (5) reduce the financial leverage China holds over the U.S. The NTSPS will create new legal and economic levers favoring the U.S. and facilitate the restructuring of the U.S.-China relationship through legal and economic means, thus reducing the risk of using military means to achieve national security and defense policy goals.

---

[216] 48 C.F.R. § 252.204–7012 (2020).

[217] *Id.*; *see also* Robert Z. Metzger, *Incident Reporting Key to New Cybersecurity Rule*, NAT'L DEF. (Jan. 29, 2018), https://www.nationaldefensemagazine.org/articles/2018/1/29/incident-reporting-key-to-new-cybersecurity-rule.