ECONOMIC WAR GAMES: HOW U.S. TRADE POLICY AND REGULATIONS HAVE SHAPED CHINESE ECONOMIC CYBER ESPIONAGE DURING THE OBAMA, TRUMP, AND BIDEN ADMINISTRATIONS

By Jamie Seibert

INTRODUCTION*

The U.S.-China economic relationship and each country's distrust of the other have affected the cyber attacks launched by foreign actors against the United States.[1] For decades, the U.S. has accused China of rampant intellectual property theft and trade violations.[2] China, on the other hand, accuses the U.S. of abusing its dominant economic position in an effort to hinder the Chinese economy.[3] Despite these enduring issues, the two countries' economies are so intertwined that neither can expect to compete in the modern economy without the other.[4] Both the Obama and Trump administrations harnessed this economic relationship to attempt to curb foreign cyber espionage targeting the U.S.[5]

The U.S. executive branch has attempted to protect the interests of the country's private sector by creating more stringent rules governing the transfer of certain technologies to foreign countries, including China.[6] For years, these rules were limited to certain sectors of technology that had direct national security concerns, such as surveillance equipment and weapons.[7] The Obama and Trump administrations had to consider the growing challenge that developing technologies pose when crossing foreign borders: the old-school classifications are no longer broad enough to capture all technologies that implicate national security.[8] As broader rules were implemented, foreign threat actors turned to

*The topic of this paper requires certain information that is currently not available to the public at large. As such, this paper is based on information made public by the U.S. government and, in some instances, cannot be independently verified. All conclusions as to the sources of various cyber attacks mentioned herein are allegations levied by the U.S. government, and not all have been adjudicated as findings of fact.

[1] JAMES ANDREW LEWIS, EMERGING TECHNOLOGIES AND MANAGING THE RISK OF TECH TRANSFER TO CHINA 2 (2019).

[2] *Id.*

[3] Barbara Plett-Usher, *US and China trade angry words at high-level Alaska talks*, BBC NEWS (Mar. 19, 2021), https://www.bbc.com/news/world-us-canada-56452471.

[4] *See* Lewis, *supra* note 1, at 1-3.

[5] *See infra* Parts I-II.

[6] *See* Lewis at 1.

[7] *Id.*

[8] *Id.* at 10.

cyber espionage to access those technologies that could no longer be legally acquired. [9]

In 2013, after four years of Obama's consistent engagement with China's trade violations, [10] the U.S. Office of Personnel Management (OPM) experienced a devastating data breach from an unidentified foreign actor.[11] The data of millions of Americans was compromised, some of it so sensitive that it endangered CIA operatives abroad. [12] Despite the severity of the hack and the growing evidence that it had been perpetrated by actors associated with the Chinese government, the Obama administration hesitated to cast blame or take retaliatory steps, instead pursing diplomatic methods of persuasion. [13] When the Trump administration took office, it swiftly retaliated in the form of trade sanctions and restrictions.[14] Today, the OPM breach continues to play a key role in the U.S.-China trade relationship.

This paper explores the connection between the U.S.'s trade restrictions on technology transfers to China and the prevalence of Chinese-linked cyber espionage attacks on the U.S. private and public sectors. The Obama administration preferred reactive diplomatic methods, only occasionally adding further export restrictions, while the Trump administration took a harsher approach, adding broad restrictions on technology transfers to China. [15] These different approaches to the U.S.-Chinese trade relationship have had an impact on the type and severity of foreign cyber espionage attacks on U.S. companies and federal agencies.[16] Now, the Biden administration appears to be seeking to bridge the divide between the two former administrations and prevent further cyber espionage attacks by increasing the U.S.'s attack-readiness

---

[9] *Id.* at 21.

[10] OFFICE OF THE UNITED STATES TRADE REPRESENTATIVE, FACT SHEET: THE OBAMA ADMINISTRATION'S UNPRECEDENTED TRADE ENFORCEMENT RECORD (2012) (hereinafter: "Fact Sheet").

[11] Josh Fruhlinger, *The OPM hack explained: Bad security practices meet China's Captain America*, CSO (Feb. 12, 2020) https://www.csoonline.com/article/3318238/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html.

[12] *Id.*

[13] David E. Sanger & Julie Hirschfeld Davis, *Hacking Linked to China Exposes Millions of US Workers*, N.Y. TIMES (June 4, 2015) https://www.nytimes.com/2015/06/05/us/breach-in-a-federal-computer-system-exposes-personnel-data.html.

[14] Cory Bennett, *Trump talks tough on China's hacking. Why not Russia's?*, POLITICO (Jan. 28, 2017) https://www.politico.com/story/2017/01/trump-russia-china-hacking-234301.

[15] *See infra* Parts I-II.

[16] *Id.*

while maintaining many of the legal approaches used by the last administration.[17]

A. TECHNOLOGY TRANSFER RULES AND CYBER ESPIONAGE DURING THE OBAMA ADMINISTRATION

President Obama's administration spent considerable time pursuing legal action against the Chinese government at the international level for violating various international trade standards.[18] Many of these actions took place at the World Trade Organization (WTO), the main international forum for trade enforcement.[19] From 2009 to 2015, Obama filed eleven enforcement actions against China.[20] The U.S. won all of those disputes, recovering monetary damages for American businesses who had their intellectual property compromised by foreign actors.[21] The administration also filed complaints against China for illegal trade practices, such as improper taxes on exports.[22]

Many of these actions succeeded, but they were at their heart retroactive measures that could only hope to deter future bad acts and could not make whole those U.S. entities who were already harmed. The actions also only applied to very specific infractions.[23] When a trade infraction occurred, an action was filed for that particular incident.[24] When a decision was handed down, it only applied to that single occurrence.[25] While the consistency with which the Obama administration enforced infractions surely had some negative effect on the Chinese government – even if only by

---

[17] *See infra* Part III.

[18] *See* Fact Sheet, *supra* note 10.

[19] *Id.* The WTO's Dispute Settlement Body has competence to settle international disputes amongst WTO members. *See Dispute Settlement Body* https://www.wto.org/english/tratop_e/dispu_e/dispu_body_e.htm.

[20] *See* Fact Sheet, *supra* note 10.

[21] *Id.*

[22] *Id.*

[23] *Id.*

[24] *Id.*

[25] *Id.* For example, the Obama administration won a ruling against China at the WTO by arguing that China's copyright law violated provisions in the TRIPS agreement, a key international intellectual property treaty. The WTO Panel found that China's law was out of compliance with TRIPS and China was made to change their law to comply better with the treaty. *See* Panel Report, *China-Measures Affecting the Protection and Enforcement of Intellectual Property Rights*, WTO Doc. WT/DS362/R (adopted Jan. 26, 2009). In another action, the U.S. filed a complaint against China at the WTO for multiple trade infractions, arguing that the restrictions imposed on the exportation of raw materials from China violated multiple international treaties. The Panel found for the US and China was made to change their various export restrictions and taxes to better comply with its duties as a WTO member. *See* Panel Report, *China — Measures Related to the Exportation of Various Raw Materials*, WTO Doc. WT/DS294/20 (adopted Jan. 23, 2013).

bogging it down in dispute resolution proceedings – the process could not prevent future harm to U.S. businesses operating in the Chinese market.[26]

During this period of constant adjudicatory redress sought for trade infractions, evidence suggests that Chinese threat actors retaliated against the U.S. with a number of cyber attacks against the U.S. government and private corporations.[27] The OPM hack, as previously discussed, was a massive breach that compromised millions of records of highly sensitive information about Americans.[28] While many experts argue that this hack was largely political, other hacks were perpetrated against private companies in an attempt to gain access to the intellectual property that was no longer accessible through technology transfers.[29] Chinese-linked hackers stole technologies across a number of industries including encryption software, solar power, nuclear power, and aerospace.[30] This economic espionage targeted U.S. corporations for their patented technologies and trade secrets, accessing the intellectual property by cyber means rather than through the trade processes the Obama administration was attacking on the international stage.[31]

While the administration pursued resolutions of its issues with China's trade policies, it also used U.S. trade law to put pressure on other foreign adversaries.[32] The U.S. Department of Commerce regulates international technology transfers, granting licenses for transfers of technologies that are restricted by the government.[33] In response to growing Russian interference in the Crimea region of Ukraine, the Obama administration instituted a presumption of denial for licenses to export technologies to that region, other than food and medicine.[34] The presumption of denial meant that most applications for licenses would be refused, unless the applicant could overcome the presumption.[35] This was an intentional obstruction to trade that sought to punish Russia for its activities in that region.[36]

---

[26] *See* Lewis, *supra* note 1, at 16.
[27] EVAN BURKE, ET. AL., SURVEY OF CHINESE-LINKED ESPIONAGE IN THE UNITED STATES SINCE 2000 10-23 (2020).
[28] *See* Fruhlinger, *supra* note 11.
[29] *See* Lewis, *supra* note 1, at 1.
[30] *See* Burke, *supra* note 27, at 11-16.
[31] *Id. See also* Lewis, *supra* note 1, at 16.
[32] BUREAU OF INDUSTRY AND SECURITY, UNDER SECRETARY ERIC L. HIRSCHHORN REMARKS TRADE DEVELOPMENT ALLIANCE OF GREATER SEATTLE (Feb. 26, 2015).
[33] *Id.*
[34] *Id.*
[35] *Id.*
[36] *Id.*

The Obama administration chose not to extend this broad and heightened presumption to China, despite growing tension between the two countries. Instead, technology transfers to China could be licensed on a case-by-case basis, a standard that is easier for U.S. companies to meet.[37] The administration was unwilling to impose the harsh policy it applied to Russia to China despite the increasingly stressed relationship. Instead, Obama employed diplomatic solutions.

In 2015, in the wake of the OPM hack and a continued rise in economic cyber espionage, Obama met President Xi Jinping of China, seeking an agreement between the two countries to cease, or at least limit, cyber attacks against each other.[38] During a state visit, Obama and President Xi Jinping discussed the countries' related goals for trade and came to an agreement to lessen the attacks perpetrated against the U.S.[39] The description of the agreement differed when presented from each country's perspective, but there was a consensus that each country would take steps to reduce cyber espionage against the other.[40] Both countries agreed not to "conduct or knowingly support cyber-enabled theft of intellectual property" for commercial advantage.[41] The agreement was finalized in September 2015, just five months after OPM announced it had been hacked.[42]

Following the U.S.-Chinese Cyber Agreement, there was a noticeable reduction in foreign attacks against the U.S., especially in attacks allegedly linked to China.[43] In 2016, one year after the agreement, private cybersecurity firm FireEye reported that incidents of Chinese attacks had dropped from sixty incidents in 2013 to less than ten by May of 2016.[44] There is some suspicion that hacks did not necessarily decrease, but rather they just became more sophisticated and went undetected.[45] However, the numbers do show a short downward trend, suggesting threat actors did reduce cyber attacks during this time.[46] Obama's combined approach, leveraging international law and diplomatic means, appeared to

---

[37] CONGR. RESEARCH SERV., THE U.S. EXPORT CONTROL SYSTEM AND THE EXPORT CONTROL REFORM INITIATIVE 3 (2020).
[38] Julie Hirschfeld Davis & David Sanger, *Obama and Xi Jinping of China Agree to Steps on Cybertheft*, N.Y. TIMES (Sept. 25, 2015).
[39] *Id*.
[40] *Id*.
[41] OFFICE OF THE PRESS SECRETARY, FACT SHEET: PRESIDENT XI JINPING'S STATE VISIT TO THE UNITED STATES (Sept. 25, 2015).
[42] *Id*.
[43] Adam Segal, *The U.S.-China Cyber Espionage Deal One Year Later*, COUNCIL ON FOREIGN RELATIONS (Sept. 28, 2016).
[44] *Id*.
[45] *Id*.
[46] *Id*.

have short-term, moderate success at reducing the amount of foreign-led cyber attacks.[47]

B. TECHNOLOGY TRANSFER RULES AND CYBER ESPIONAGE DURING THE TRUMP ADMINISTRATION

After Obama's apparent diplomatic success, the Trump administration took office and quickly cast China as the adversary to U.S. economic success.[48] The administration launched an aggressive legal approach against China, releasing white papers and executive orders accusing China of hacking OPM and seeking retribution for past and continued economic cyber espionage.[49] In 2018, the administration released a report alleging China's participation in cyber espionage against U.S. companies and expounded Trump's hardline approach to solving the issue.[50] Following the report, Trump signed an executive order in 2019 that created broad restrictions on technology transfers with China and other foreign adversaries.[51]

The Order was the first step to creating widespread restraints on technology transfers to China.[52] The Order banned any technology transfer with a citizen of a "foreign adversary" and which federal agencies found posed an "unacceptable risk" to national security or U.S. interests.[53] The language is broad, and left much of the determinations up to federal agencies, including the departments of Commerce and Defense, and the U.S. Trade Representative.[54] The Order carved out an exception for those technology transfers that have a license to operate.[55] These licenses are granted by agencies like the Department of Commerce, so the exception acted to grant more power to federal agencies to determine which transactions were appropriate.[56] This wide delegation of power allowed agencies to create rules that swept in

---

[47] *Id.*
[48] WHITE HOUSE OFFICE OF TRADE AND MANUFACTURING POLICY, HOW CHINA'S ECONOMIC AGGRESSION THREATENS THE TECHNOLOGIES AND INTELLECTUAL PROPERTY OF THE UNITED STATES AND THE WORLD (June 2018) (hereinafter "Trump China IP Report").
[49] David E. Sanger & Steven Lee Myers, *After a Hiatus, China Accelerates Cyberspying Efforts to Obtain U.S. Technology*, N.Y. TIMES (Nov. 29, 2018). *See e.g.*, Trump China IP Report, *supra* note 48. *See also* Exec. Order No. 13873 (2019). *See also* Exec. Order No. 13920 (2020).
[50] *See* Trump China IP Report, *supra* note 48.
[51] Exec. Order No. 13873 (2019).
[52] *Id.*
[53] *Id.*
[54] *Id.*
[55] *Id.*
[56] *Id.*

technologies from a variety of industries not traditionally considered relevant to national security.[57]

The U.S. has long restricted technology transfers that could impact national security.[58] The restrictions operate to prevent technologies that could benefit a foreign military from falling into its hands, and so were traditionally limited to technologies, such as weapons, that could explicitly and directly benefit other nations.[59] A change in the export rules' language expanded these restriction to new technologies by changing the focus from considering just the buyer and seller party to the transaction.[60] The amended rule focused on the end use, rather than the seller's intended use, of the goods.[61] Sellers might once have been able to transfer a technology—like a patented solar power mechanism—to a privately-owned Chinese company, but under the amended rule, the Bureau of Industry and Security (BIS), when considering the approval of the transaction, would look beyond the Chinese company and try to determine how the technology would eventually be used and by whom.[62] Even if the seller is only transferring the technology to a private enterprise, the federal agency might decide that the final end use is actually to benefit the Chinese military, based on the buyer-company's relationship with the Chinese government.[63] The agency could then refuse a license and prevent the transaction from taking place.[64] This is a major expansion of the technology transfer review process and resulted in widespread restrictions on trade with Chinese private entities.[65]

In addition to this new review process, Trump's agencies also amended the legal standard under which export requests are reviewed by BIS.[66] Under previous administrations, each export license request for technology transfers to China was examined on a case-by-case basis.[67] The new rule issued under Trump instead created a presumption of denial for technology transfer licenses to Chinese entities, making it much more difficult for U.S. transferors

---

[57] US INTERNATIONAL TRADE ADMINISTRATION, CHINA - COUNTRY COMMERCIAL GUIDE: US EXPORT CONTROLS 4 (Feb. 2, 2021) (hereinafter "Trump China Export Controls").
[58] *Id*.
[59] Burt Braverman & Brian Wong, *New Rules Restrict U.S. Exports to China, Targeting Chinese Military End Uses and End Users*, (May 19, 2020) https://www.dwt.com/insights/2020/05/us-bis-china-technology-export-ban.
[60] *Id*.
[61] *Id*.
[62] *Id*.
[63] *Id*.
[64] *Id*.
[65] *Id*.
[66] *See* Trump China Export Controls, *supra* note 57, at 4.
[67] *See* Braverman, *supra* note 59.

to be granted a license.[68] BIS issued guidance on the change and anticipated a "continuing likelihood of denials" of export licenses for transactions with China, implying that the rule existed with the intention to prevent most transactions from taking place.[69]

The presumption of denial cut across industries, sweeping into its breadth traditional military technologies, but also more broad technologies and supply chains that would, under the previous standard, have been granted a license.[70] The combination of the expansion of licenses based on the goods' end use and the presumption of denial meant that the vast majority of technology transfers, even those outside the scope of traditional military technology, were subjected to a tougher standard.[71] All of this resulted in large restraints on trade with China, harming China's ability to access key sectors of technology it could have accessed before the amended rules.[72]

In addition to the changes to the export rules, agencies issued more regulations governing technology transfers with private Chinese businesses and individuals, and among those regulations was a growing list of companies to whom U.S. citizens could no longer transfer many types of technologies.[73] Ever since entering the Chinese market, the U.S. has kept a list of banned entities with whom U.S. companies cannot trade.[74] However, under the Trump administration, that list of entities grew far more quickly than under previous administrations.[75] During his presidency, the Trump administration added more entities to the restricted list than the Bush administration did during its eight-year tenure, and added more than double the number of entities than did the Obama administration.[76] BIS added key Chinese technology companies, such as Huawei,[77] to the list of restricted entities.[78] It then added more than 100 Huawei affiliates to the list, making an aggressive stand against some of the Chinese economy's biggest technology companies and their coordination with U.S. companies.[79] These widespread restrictions

---

[68] *See* Trump China Export Controls, *supra* note 57, at 4.
[69] *See* Braverman, *supra* note 59.
[70] *Id.*
[71] *Id.*
[72] *Id.*
[73] Judith Alison Lee, et. al., *2020 Year-End Sanctions and Export Controls Update*, (Feb. 5, 2021) https://www.gibsondunn.com/wp-content/uploads/2021/02/2020-year-end-sanctions-and-export-controls-update.pdf.
[74] *Id.*
[75] *Id.*
[76] *Id.*
[77] *Id.*
[78] *Id.*
[79] *Id.*

on trade had the desired effect: technology transfers from the U.S. to China were far more difficult to effectuate.[80]

These changes harmed U.S. trade with China, and soon after the changes were enacted, it seemed Chinese-linked threat actors retaliated with a marked increase in cyber attacks on the U.S. economy.[81] After an 18-month decline in cyber incidents following the 2015 economic cyber espionage agreement under the Obama administration, the U.S. private sector experienced a number of large economic cyber espionage attacks.[82] The sophisticated attacks targeted U.S. companies that owned coveted technologies, and some experts have argued that these attacks purposefully sought access to those technologies that were no longer available through technology transfers, such as aerospace, artificial intelligence, and quantum computing technologies.[83] The hacks that took place during this period were assumed to be both politically and economically motivated.[84] Many argue that hackers sought to access technologies they could no longer obtain through trade in an effort to bolster the Chinese economy while also exacting pain on U.S. companies in retaliation for the Trump administration's harsh trade approach.[85]

One of the most substantial hacks during this period was the 2018 attack on Marriott that resulted in the breach of nearly 500 million guests' data.[86] This hack exemplifies the dual political and economic goals of foreign actors' hacks: Marriott is not only a large U.S. company with ample IP at risk, but it is also the main hotel provider for U.S. government and military personnel.[87] The hack compromised sensitive information like passport data, and experts speculate that the Chinese government could use this information to track Americans' movements and travel plans.[88] The timing of this hack had immediate political significance, as it was announced at the same time the U.S. was negotiating a $1.2 trillion trade deal with China that attempted to address concerns over IP theft.[89] The hack of Marriott led many experts to agree that the cooling-off experienced under the 2015 Obama-era agreement had come to an end.[90]

---

[80] *Id*.
[81] *See* Sanger, *supra* note 49.
[82] *Id*.
[83] *Id*.
[84] *Id*.
[85] *Id*.
[86] David E. Sanger, et. al., *Marriott Data Breach is Traced to Chinese Hackers as U.S. Readies Crackdown on Beijing*, N.Y. TIMES (Dec. 11, 2018).
[87] *Id*.
[88] *Id*.
[89] *Id*.
[90] *Id*.

The amount of cyber attacks did not decline even after Trump lost his bid for re-election in 2020.[91] The COVID-19 crisis worsened relations as the Trump administration openly blamed China for the worldwide pandemic and its effect on the U.S. economy. [92] Foreign hacks remained effective, targeting U.S. defense contractors, developers, and researchers.[93] In May of 2020, U.S. officials linked Chinese hackers to an attempted breach of U.S. research into a COVID-19 vaccine.[94] The Trump administration's handling of the pandemic increased tensions with China, resulting in worsened relations that the newly-installed Biden administration is currently facing.[95]

C. PREDICTING THE BIDEN ADMINISTRATION TRADE RESPONSE TO CONTINUED CHINESE CYBER ESPIONAGE

Following four tense years of aggression against China under the Trump administration, the Biden administration inherited a U.S.-China relationship that is defined by open hostility.[96] Cyber attacks did not decrease during the transition to the new administration,[97] and the Biden administration continues to use methods of deterrence "when it's in America's interest to do so."[98] Although the Biden administration will likely seek a return to the kind of globalization achieved under Obama's tenure, the elusive goal of open trade is tempered by a strategy that requires engagement with adversaries when diplomatic means are insufficient.[99]

The first one-hundred days of Biden's presidency were marked by cyber attacks on government contractors and other private entities,[100] and while Biden has signaled he intends to pursue

---

[91] *See* Burke, *supra* note 27, at 33-34.
[92] Scott Neuman, *In U.N. Speech, Trump Blasts China and WHO, Blaming Them for Spread of COVID-19*, NPR (Sept. 22, 2020) https://www.npr.org/sections/coronavirus-live-updates/2020/09/22/915630892/in-u-n-speech-trump-blasts-china-and-who-blaming-them-for-spread-of-covid-19.
[93] SIGNIFICANT CYBER INCIDENTS, Center for Strategic and International Studies (April 2021).
[94] *Id.* at 20.
[95] *See* Neuman, *supra* note 92.
[96] Jonathan Marcus, *US-China relations: Beyond the 'Cold War' cliché*, BBC NEWS (Mar. 17, 2021) https://www.bbc.com/news/world-asia-56382793.
[97] *See* Burke, *supra* note 27, at 33-34.
[98] WHITE HOUSE BRIEFING ROOM: REMARKS BY PRESIDENT BIDEN ON AMERICA'S PLACE IN THE WORLD (Feb. 4, 2021).
[99] *Id*.
[100] *See e.g.* Kevin Collier, *China behind another hack as U.S. cybersecurity issues mount*, NBC NEWS (April 21, 2021) https://www.nbcnews.com/tech/security/china-another-hack-us-cybersecurity-issues-mount-rcna744.

diplomatic solutions to the tense Chinese-U.S. relationship, he has also used strong language that indicates he will attempt to meld the strategies used by his two most recent predecessors.[101] In statements to the press in early February 2021, National Security Advisor Jake Sullivan resisted insinuations that the Biden administration would take a purely diplomatic approach to cyber attacks from foreign entities, implying the administration would pair diplomacy with harsher, retaliatory acts against foreign adversaries.[102] This attitude is sharper than the strict diplomatic approach Obama employed, but also softer than the "America First" logic that drove the Trump administration.

Thus far, cyber attacks have not relented during the start of Biden's term.[103] In the first weeks of his presidency, two large-scale attacks became public.[104] First, U.S. law enforcement agencies attributed the hack of the defense contractor SolarWinds to the Russian government.[105] The severity of this hack is still being studied, but it dominated headlines during a time when Biden was attempting to initiate his cyber strategy.[106] Another large hack was that of Microsoft, where the U.S. accused hackers associated with China of exploiting a gap in the Microsoft Exchange email service.[107] These are both large-scale hacks that show foreign adversaries did not stop cyber attacks during the transition between administrations.[108]

In an acknowledgement of the increased danger of cyber espionage, Biden has established a cyber-bureaucracy with the intention of creating stronger cybersecurity protections within the government.[109] He appointed a Deputy for Cyber and Emerging Technology, Anne Neuberger, who now serves on the National Security Counsel advising on the cyber risks facing the government and private entities.[110] Biden continued to build this bureaucratic structure to support his cyber strategy through additional appointments, such as those of Jen Easterly (head of the cybersecurity unit housed under Homeland Security) and John Inglis (National Cyber Director, a new function housed in the White

---

[101] *See* White House Briefing Room, *supra* note 98.
[102] *Id.*
[103] David P. Fidler, *America's Place in Cyberspace: The Biden Administration's Cyber Strategy Takes Shape*, COUNCIL ON FOREIGN RELATIONS (Mar. 11, 2021).
[104] *Id.*
[105] *Id.*
[106] *Id.*
[107] *Id.*
[108] *Id.*
[109] Zach Whittaker, *Biden's cybersecurity dream team takes shape*, TECHCRUNCH (April 12, 2021) https://techcrunch.com/2021/04/12/bidens-cybersecurity-dream-team-takes-shape/.
[110] *Id.*

House). [111] The string of appointments shows the Biden administration is leveling up its cybersecurity teams, setting the stage for stronger security that can respond to attacks.[112] It also signals to foreign adversaries that the U.S. is prepared to retaliate should an attack occur.[113] The increase in administrative cyber expertise showcases Biden's cyber strategy: increasing security strength as a measure to protect and actively deter future attacks.[114]

As Biden built his administration's cyber-infrastructure, his administration also moved to harness the power of international trade restrictions to keep pressure on China.[115] Despite a return to diplomacy, Biden's U.S. Trade Representative (USTR) has kept China on its "priority watchlist" of nations that require extra monitoring for trade violations.[116] Though Biden often criticized the Trump trade-war approach to China, the report from the USTR signals that the administration will maintain many of the broad export restrictions leftover from the Trump administration.[117]

Looking to how Biden has engaged with other foreign adversaries following cyber attacks, we can predict how he might engage with China during his presidency. After the Russian attack on SolarWinds, and in retaliation for Russia's interference in U.S. elections, the administration imposed "seen and unseen" sanctions on Russia.[118] The "unseen" measures may never be publicly known, but it is predicted that the administration plans to launch cyber operations against those responsible for the SolarWinds hack.[119] The "seen" sanctions include blocking U.S. financial institutions from granting bonds to key Russian banks and fining six Russian tech companies who are known for providing support to Russian intelligence operations.[120] These sanctions seek to punish Russia for its actions by hitting the country where it hurts: international trade and financial operations.[121] Although Biden has not yet taken steps

---

[111] *See* Whittaker, *supra* note 109.
[112] *Id.*
[113] PRESS BRIEFING BY PRESS SECRETARY JEN PSAKI AND DEPUTY NATIONAL SECURITY ADVISOR FOR CYBER AND EMERGING TECHNOLOGY ANNE NEUBERGER (Feb. 17, 2021) (hereinafter "Neuberger Press Briefing").
[114] *Id.*
[115] OFFICE OF THE US TRADE REPRESENTATIVE, 2021 SPECIAL 301 REPORT 40 (April 2021).
[116] *Id.*
[117] *Id.*
[118] Morgan Chalfant & Maggie Miller, *Biden administration sanctions Russia for SolarWinds hack, election interference*, THE HILL (April 15, 2021) https://thehill.com/homenews/administration/548367-biden-administration-unveils-sweeping-sanctions-on-russia.
[119] *Id.*
[120] *Id.*
[121] *Id.*

to remove or bolster the broad trade restrictions on business with Chinese entities, his actions toward Russia show a hardline approach that could be applied to the U.S.-China trade relationship.

Although the administration's trade approach has not yet been publicly released, it is worthwhile to note the legal options Biden may pursue in his efforts to deter foreign cyber espionage. His campaign often criticized the Trump administration's tactics,[122] so Biden may seek to cool off the relationship by loosening some trade restrictions. Reversing the presumption of denial for technology transfer licenses would promote trade between the countries' private sectors and return the agency's stance to that employed under the Obama administration.[123] Without this policy, U.S. companies applying for technology transfer licenses would no longer have to rebut the presumption, making it easier for licenses to be granted and technology transfers to take place. While this might seem like a step back from the strong rhetoric the administration has used thus far, it could still be powerful if the Biden administration continues to add problematic Chinese companies to the BIS Entities List.[124] Then, those companies that are not threats can more easily trade with the U.S., but those that remain dangerous will continue to be banned. This could improve relations while still protecting the U.S. private sector. By balancing these legal options, the Biden administration could maintain a strong position on China while still permitting U.S. entities to transfer technologies.

A tough approach to China was used by the previous administration, but the current administration appears to aim at pairing that strong rhetoric with a strengthened cyber-infrastructure for the federal government and private sector.[125] So far, it is not clear that Biden's strategy is working. China has remained on trade watchlists and the presumption of denial for technology transfers with many Chinese businesses has not yet been removed.[126] To strengthen the country's cyber defenses, Biden asked for ample funds from Congress and appointed top cybersecurity experts to key bureaucratic positions.[127] Still, the cyber attacks have not stopped.[128] What remains to be proven is whether the administration

---

[122] Jim Zarroli, *Trump Launched a Trade War Against China. Don't Look to Biden to Reverse It*, NPR (Nov. 18, 2020) https://www.npr.org/2020/11/18/935718860/trump-launched-a-trade-war-against-china-dont-look-to-biden-to-reverse-it.
[123] *See* CONGR. RESEARCH SERV., *supra* note 37.
[124] *See supra* Part II, discussing the BIS entities list.
[125] *See* Neuberger Press Briefing, *supra* note 113.
[126] *See supra* discussion accompanying notes 115-17.
[127] *See* Whittaker, *supra* note 109.
[128] *See* Significant Cyber Incidents, *supra* note 93.

can harness the legal tools discussed, to foster a better relationship with Chinese businesses while still keeping pressure on the Chinese government to deter future cyber espionage.

CONCLUSION

Obama tried diplomacy.[129] Trump tried a trade war.[130] Now, Biden is attempting to strike a balance between the two strategies that can punish foreign adversaries for cyber espionage of protected technologies and deter future attacks.[131] With numerous legal tools at his disposal - from sanctions, to the BIS Entities List, to international arbitration - Biden could harness China's reliance on the U.S. economy to improve its protection of the U.S. private sector.[132] When the U.S. cracks down too hard on China's access to technologies, an increase in cyber espionage attacks seems to follow.[133] The Biden administration can only hope to deter these attacks by strengthening the U.S.'s cyber-defense mechanisms and cooling down the tense U.S.-China relationship. Now, nearly one year into his presidency, Biden should employ the trade laws at his disposal to encourage legitimate technology transfers while protecting the U.S. from further cyber economic espionage.

---

[129] *See supra* Part I.
[130] *See supra* Part II.
[131] *See* Fidler, *supra* note 103.
[132] *See supra* discussion accompanying notes 122-25.
[133] *See* Lewis, *supra* note 1, at 21.