V. Unauthorized Intrusions into U.S. Commercial Computer Networks and Cyber-Enabled Theft of Intellectual Property and Sensitive Commercial Information

A. Introduction

For over a decade, the Chinese government has conducted and supported cyber intrusions into U.S. commercial networks targeting confidential business information held by U.S. firms. Through these cyber intrusions, China's government has gained unauthorized access to a wide range of commercially-valuable business information, including trade secrets, technical data, negotiating positions, and sensitive and proprietary internal communications. These acts, policies, or practices by the Chinese government are unreasonable or discriminatory and burden or restrict U.S. commerce.

Section V.B of this report will first detail the cyber actions taken by the Chinese government against U.S. companies including the theft of confidential business information that would have provided a competitive economic advantage. Section V.B will then analyze how the Chinese government's cyber intrusions support its industrial policy goals and how this activity has continued in recent years. Section V.C concludes that China's actions are unreasonable and Section V.D explains the economic burden on and harm felt by targeted U.S. companies.

Experts have acknowledged that China's cyber activities represent a grave threat to U.S. competitiveness and the U.S. economy. Starting in 2008, experts expressed concern that China's cyber intrusions were becoming more frequent, more targeted, and more sophisticated.[967] As one expert has noted, "[w]hereas before the activities were targeted at government and military networks…, the new intrusions went beyond state-on-state espionage to threaten American technological competitiveness and economic prosperity."[968] The Office of the National Counterintelligence Executive added in 2011 that "Chinese actors are the world's most active and persistent perpetrators of economic espionage."[969]

As discussed in more detail below, evidence from U.S. law enforcement and private sources indicates that the Chinese government has used cyber intrusions to serve its strategic economic objectives. Documented incidents of China's cyber intrusions against U.S. commercial entities align closely with China's industrial policy objectives. As the global economy has increased its dependence on information systems in recent years, cyber theft became one of China's preferred methods of collecting commercial information because of its logistical advantages and plausible deniability.[970]

---

[967] See *e.g.*, Shane Harris, *China's Cyber Militia*, NAT'L J., May 31, 2008. (citing remarks of a senior official from the U.S. Director of National Intelligence).

[968] HANNAS, ET AL., CHINESE INDUSTRIAL ESPIONAGE: TECHNOLOGY ACQUISITION AND MILITARY MODERNIZATION, 217 (2013).

[969] OFFICE OF THE NATIONAL COUNTERINTELLIGENCE EXECUTIVE, FOREIGN SPIES STEALING US ECONOMIC SECRETS IN CYBERSPACE: REPORT TO CONGRESS ON FOREIGN ECONOMIC COLLECTION AND INDUSTRIAL ESPIONAGE, 2009-2011 i (Oct. 2011).

[970] A number of public submissions provided to USTR state that the Chinese government has no reason to conduct cyber intrusions or commit cyber theft for commercial purposes, *see* CHINA GENERAL CHAMBER OF COMMERCE [*hereinafter* "CGCC"], *Submission, Section 301 Hearing* 16 (Sept. 28, 2017); that the US has not provided evidence of such actions by China, that China is also a target of cyberattacks, and that the two countries should work together

V. Unauthorized Intrusions into U.S. Commercial Computer Networks and Cyber-Enabled Theft of Intellectual Property and Sensitive Commercial Information

The Chinese and American presidents reached a commitment on refraining from the cyber-enabled theft of intellectual property (IP) and other confidential business information for commercial advantage in September 2015.[971] The United States has been closely monitoring China's cyber activities and the evidence indicates that China continues its policy and practice, spanning more than a decade, of using cyber intrusions to target U.S. firms to access their sensitive commercial information and trade secrets. For example, as described in more detail below, in September 2017 the U.S. Department of Justice filed an indictment against Chinese nationals for intruding into U.S. commercial networks and stealing commercially sensitive information. Cybersecurity firms have linked the firm for which these individuals worked to the Chinese government.[972]

Because cyber intrusions depend on deception and obfuscation, the acts, policies, and practices at issue by their nature impair the comprehensive collection and analysis of all relevant information. Businesses are often unaware that their computer networks have been compromised by an infiltration,[973] and those that are aware of such intrusions are often apprehensive about sharing publicly the details of any compromise. Accordingly, this report has drawn upon information in the public domain from both private parties and U.S. law enforcement. However, publicly available information necessarily represents only a fraction of all relevant activity.

B. China's Acts, Policies, and Practices Regarding Unauthorized Intrusions into U.S. Commercial Computer Networks and Cyber-Enabled Theft of Intellectual Property and Sensitive Commercial Information

1. The Chinese Government's Extensive Cyber Activities

The Chinese government's cyber intrusions into U.S. firms' networks have been well documented by private cybersecurity companies. For example, McAfee's 2011 *Night Dragon* report documents advanced persistent threat, or APT, activity from China against global oil, energy, and petrochemical companies "targeting and harvesting sensitive competitive proprietary operations and project-financing information with regard to oil and gas field bids and operations."[974]

---

to address cybersecurity issues. *See* CHINA CHAMBER OF INTERNATIONAL COMMERCE [*hereinafter* "CCOIC"], *Submission, Section 301 Hearing* 68-70 (Sept. 39, 2017); CHINA CHAMBER OF COMMERCE FOR IMPORT AND EXPORT OF MACHINERY AND ELECTRONIC PRODUCTS [*hereinafter* "CCCME"], *Submission, Section 301 Hearing* 12 (Sept. 27, 2017). The discussion and accompanying references that follow establish a record of China's cyber intrusions and cyber theft. That China may also be a target of cyberattack is outside the scope of this investigation.

[971] Press Release, The White House, Fact Sheet: President Xi Jinping's State Visit to the United States (Sept. 25, 2015).

[972] INSIKT GROUP, *Recorded Future Research Concludes Chinese Ministry of State Security Behind APT3,* RECORDED FUTURE (May 17, 2017) (last visited Jan. 10, 2018).

[973] *See* VERIZON, 2017 DATA BREACH INVESTIGATIONS REPORT (2017).

[974] MCAFEE FOUNDSTONE PROFESSIONAL SERVICES & MCAFEE LABS, GLOBAL ENERGY CYBER ATTACKS: "NIGHT DRAGON" 3 (Feb. 10, 2011).

V. Unauthorized Intrusions into U.S. Commercial Computer Networks and Cyber-Enabled Theft of Intellectual Property and Sensitive Commercial Information

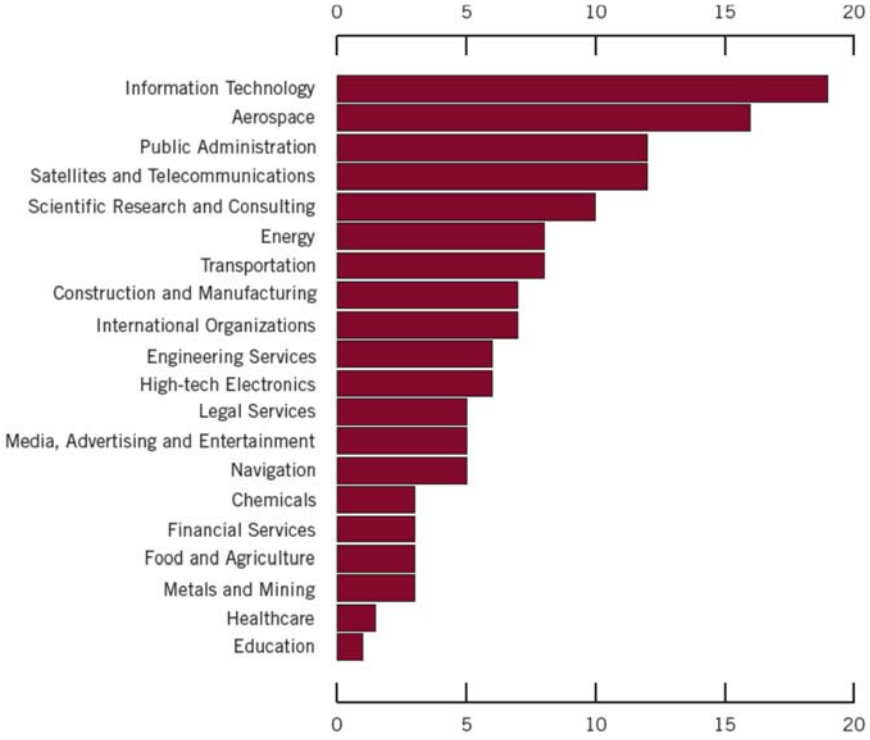
Verizon's 2013 *Data Breach Investigations Report* concluded that "State-affiliated actors tied to China are the biggest mover in 2012. Their efforts to steal IP comprise about one-fifth of all breaches in this dataset."[975] Moreover, 95% of the espionage cases[976] in the dataset were attributed to threat actors in China, which "may mean that other threat groups perform their activities with greater stealth and subterfuge. But it could also mean that China is, in fact, the most active source of national and industrial espionage in the world today."[977]

In 2013, the cybersecurity firm Mandiant released a detailed report connecting the theft of hundreds of terabytes of data by China's People's Liberation Army (PLA) General Staff Department, Third Department (3PLA), Second Bureau— a signals intelligence component of the PLA, known by its Military Unit Cover Designation as Unit 61398[978] and referred to by Mandiant as "Advanced Persistent Threat 1" or "APT1."[979] At the time of the report, Mandiant estimated that Unit 61398 was "staffed by hundreds, and perhaps thousands of people based on the size of Unit 61398's physical infrastructure."[980] The report includes details on more than 3,000 indicators associated with APT1 and Mandiant's attribution of the cyber incidents to the 3PLA.[981]

[975] VERIZON, 2013 DATA BREACH INVESTIGATIONS REPORT 5 (2013) ("State-affiliated actors tied to China are the biggest mover in 2012. Their efforts to steal IP comprise about one-fifth of all breaches in this dataset.").
[976] The report defined this as "state-sponsored or affiliated actors seeking classified information, trade secrets, and intellectual property in order to gain national, strategic, or competitive advantage". VERIZON, 2013 DATA BREACH INVESTIGATIONS REPORT 11 (2013).
[977] VERIZON, 2013 DATA BREACH INVESTIGATIONS REPORT 21 (2013).
[978] MANDIANT, APT1: EXPOSING ONE OF CHINA'S CYBER ESPIONAGE UNITS 3 (2013); *see also* Mark Stokes, PROJECT 2049 INSTITUTE, THE PLA GENERAL STAFF DEPARTMENT THIRD DEPARTMENT SECOND BUREAU: AN ORGANIZATIONAL OVERVIEW OF UNIT 61398, 3-4 (July 27, 2015) ("Signals intelligence (SIGINT), or technical reconnaissance in PLA lexicon, advances the interests of the Chinese Communist Party (CCP) and the People's Republic of China (PRC). The PLA's SIGINT community consists of at least 28 technical reconnaissance bureaus (TRBs)… The Second Bureau (Unit 61398) is one of the largest among the 12 operational bureaus that comprise the GSD Third Department.").
[979] An "APT" or "Advanced Persistent Threat" uses multiple phases to break into a computer network, avoid detection, and harvest valuable information over the long term. *Advanced Persistent Threats: How They Work*, SYMANTEC, https://www.symantec.com/theme.jsp?themeid=apt-infographic-1 (last visited Jan. 10, 2018).
[980] MANDIANT, APT1: EXPOSING ONE OF CHINA'S CYBER ESPIONAGE UNITS 3 (2013).
[981] MANDIANT, APT1: EXPOSING ONE OF CHINA'S CYBER ESPIONAGE UNITS 5 (2013).

V. Unauthorized Intrusions into U.S. Commercial Computer Networks and Cyber-Enabled Theft of Intellectual Property and Sensitive Commercial Information

According to Mandiant, this unit of the 3PLA stole data from at least 141 organizations, 115 of which are based in the United States, representing 20 major business sectors. The victims of these intrusions match industries that China has identified as strategic priorities, including four of the seven "strategic emerging industries" that China identified in its 12th Five-year Plan.[982] The table below illustrates the number of 3PLA victims by sector in Mandiant's data set.



Source: MANDIANT APT1: EXPOSING ONE OF CHINA'S CYBER ESPIONAGE UNITS

Mandiant identified a wide range of commercial sector targets of 3PLA, including information technology, energy, financial services, food and agriculture, metals and mining, electronics, and chemicals. According to the report, 3PLA has stolen a wide range of sensitive commercial information from these victims including:

- product development and use, including information on test results, system designs, product manuals, parts lists, and simulation technologies;
- manufacturing procedures, such as descriptions of proprietary processes, standards, and waste management processes;
- business plans, such as information on contract negotiation positions and product pricing, legal events, mergers, joint ventures, and acquisitions;
- policy positions and analysis, such as white papers, and agendas and minutes from meetings involving high ranking personnel;
- e-mails of high-ranking employees; and

[982] MANDIANT, APT1: EXPOSING ONE OF CHINA'S CYBER ESPIONAGE UNITS 3, 24 (2013).

- user credentials and network architecture information.[983]

The Mandiant report suggests that a reasonable inference from the evidence it has collected is that intrusions conducted by this unit of the 3PLA supported commercial interests in China. For example, the report points to a company involved in a wholesale industry whose network was compromised by 3PLA for over two and half years. During this time, 3PLA reportedly stole countless files from the victim.[984] According to the report, the 3PLA unit repeatedly accessed the e-mail accounts of several executives, including the CEO and General Counsel.[985] The Mandiant report states that at the same time as these intrusions were occurring:

> [M]ajor news organizations reported that China had successfully negotiated a double-digit decrease in price per unit with the victim organization for one of its major commodities. This may be coincidental; however, it would be surprising if APT1 could continue perpetrating such a broad mandate of cyber espionage and data theft if the results of the group's efforts were not finding their way into the hands of entities able to capitalize on them."[986]

2. The United States Department of Justice Indicted Chinese Government Hackers in May 2014

In May 2014, the United States Department of Justice (DOJ) announced an indictment against five 3PLA officers for cyber intrusions and economic espionage directed against U.S. firms.[987] These five officers were assigned to 3PLA's Second Bureau, Unit 61398, which Mandiant had identified as APT1 the year prior.[988] The 3PLA officers were charged with cyber intrusions into the computer networks of six U.S. victims: Westinghouse Electric Company (Westinghouse), SolarWorld Americas, Inc. (SolarWorld), United States Steel Corporation (U.S. Steel), Allegheny Technologies, Inc. (ATI), Alcoa Inc. (Alcoa), and the United Steel, Paper and Forestry, Rubber, Manufacturing, Energy, Allied Industrial and Services Workers International Union (USW).[989]

The intrusions by the 3PLA were conducted at times when each of the victims had a significant business relationship or business issue with China.[990] In addition, each of the victims operate in a sector that the Chinese government has prioritized for development.[991] The indictment alleges

---

[983] MANDIANT, APT1: EXPOSING ONE OF CHINA'S CYBER ESPIONAGE UNITS 25 (2013).
[984] MANDIANT, APT1: EXPOSING ONE OF CHINA'S CYBER ESPIONAGE UNITS 25 (2013).
[985] MANDIANT, APT1: EXPOSING ONE OF CHINA'S CYBER ESPIONAGE UNITS 25 (2013).
[986] MANDIANT, APT1: EXPOSING ONE OF CHINA'S CYBER ESPIONAGE UNITS 25 (2013).
[987] U.S. v. Wang Dong et al., (W. D. Pa. May 1, 2014) (Crim. No. 14-118 W.D.Pa.); *see also* Mark Stokes, PROJECT 2049 INSTITUTE, THE PLA GENERAL STAFF DEPARTMENT THIRD DEPARTMENT SECOND BUREAU: AN ORGANIZATIONAL OVERVIEW OF UNIT 61398, 3 (July 27, 2015).
[988] *See* Mark Stokes, PROJECT 2049 INSTITUTE, THE PLA GENERAL STAFF DEPARTMENT THIRD DEPARTMENT SECOND BUREAU: AN ORGANIZATIONAL OVERVIEW OF UNIT 61398 (July 27, 2015); *see also* MANDIANT, APT1: EXPOSING ONE OF CHINA'S CYBER ESPIONAGE UNITS 3 (2013).
[989] U.S. v. Wang Dong et al., 4-8 (W. D. Pa. May 1, 2014).
[990] U.S. v. Wang Dong et al., 13-26 (W. D. Pa. May 1, 2014).
[991] *See e.g.*, *The Plan for the Adjustment and Revitalization of the Steel Industry* (State Council, published Mar. 20, 2009); *12th Five-year Steel Industry Development Plan* (MIIT, Gong Xin Bu Gui [2011] No. 480, issued Oct. 24,

that "the defendants conspired to hack into American entities, to maintain unauthorized access to their computers and to steal information from those entities that would be useful to their competitors in China, including state-owned enterprises (SOEs)."[992] In some cases, the indictment alleges that the defendants stole trade secrets that "would have been particularly beneficial to Chinese companies at the time they were stolen."[993] In other cases, the indictment alleges that the defendants "stole sensitive, internal communications that would provide a competitor, or an adversary in litigation, with insight into the strategy and vulnerabilities of the American entity."[994] Meanwhile, during the period relevant to the cyber intrusions, the indictment states:

> Chinese firms hired the same PLA Unit where the defendants worked to provide information technology services. For example, one SOE involved in trade litigation against some of the American victims mentioned herein hired the Unit, and one of the co-conspirators charged herein, to build a 'secret' database designed to hold corporate 'intelligence'.[995]

a) SolarWorld

The indictment alleges that in 2012, while SolarWorld was litigating a petition it had filed against solar imports from China, the 3PLA stole thousands of sensitive files from SolarWorld. According to the indictment, these files included:

> (1) cash-flow spreadsheets maintained by the Chief Financial Officer that would enable a Chinese competitor to identify the length of time that SolarWorld might survive a financial or market shock; (2) detailed manufacturing metrics, technological innovations, and production line information that would enable a Chinese competitor to mimic SolarWorld's proprietary production capabilities without the need to invest time or money in research and development; (3) specific production costs for all manufacturing inputs that would enable a Chinese competitor to undermine SolarWorld financially through targeted and sustained underpricing of solar products; and (4) privileged attorney-client communications related to SolarWorld's ongoing trade litigation with

2011); *12th Five-year Solar Power Development Plan*, (NEA, Guo Neng Xin Neng [2012] No. 194, issued July 7, 2012); *Medium-Long Term Nuclear Power Development Plan* (NDRC, issued Oct. 2007).

[992] Press Release, Department of Justice, U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage (May 19, 2014), *available at* https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

[993] Press Release, Department of Justice, U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage (May 19, 2014), *available at* https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

[994] Press Release, Department of Justice, U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage (May 19, 2014), *available at* https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

[995] U.S. v. Wang Dong et al., 3 (W. D. Pa. May 1, 2014).

V. Unauthorized Intrusions into U.S. Commercial Computer Networks and Cyber-Enabled Theft of Intellectual Property and Sensitive Commercial Information

China, including confidential Question and Answer documents submitted to the Department of Commerce that were not discoverable by the Chinese respondents.[996]

According to DOJ, "such information would have enabled a Chinese competitor to target SolarWorld's business operations aggressively from a variety of angles.[997]

The indictment alleges that data were stolen from SolarWorld on at least twelve occasions, including during the following the incidents:

- On May 3 and May 9, 2012, the 3PLA stole files and e-mails from SolarWorld employees, including three senior SolarWorld executives.[998] The May 3 cyber intrusion occurred one day after the Coalition for American Solar Manufacturing led by SolarWorld issued a public analysis criticizing China's new Five-year Plan for Solar Photovoltaic Industry[999] and about two weeks before the U.S. Department of Commerce announced its preliminary determination in a trade complaint SolarWorld had filed against Chinese producers of solar cells.[1000]

- On July 27, 2012, the 3PLA stole e-mails and files belonging to five employees,[1001] just two days after SolarWorld's parent company filed a trade complaint with the European Commission against Chinese producers of solar modules and components.[1002]

- Between May 9 and September 26, 2012, the 3PLA conducted at least twelve more intrusions into and exfiltrations from SolarWorld's computers.[1003] The intrusion on September 26, 2012 occurred on the same day that SolarWorld filed a second trade complaint against Chinese solar products with the European

[996] U.S. v. Wang Dong et al., 18 (W. D. Pa. May 1, 2014).
[997] Press Release, Department of Justice, U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage (May 19, 2014), *available at* https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.
[998] U.S. v. Wang Dong et al., 17, 34, 35 (W. D. Pa. May 1, 2014).
[999] COALITION FOR AMERICAN SOLAR MANUFACTURING, ANALYSIS: CHINA'S NEW FIVE-YEAR PLAN FOR SOLAR CALLS FOR ESCALATION IN GOVERNMENT SPONSORSHIP OF EXPORT-INTENSIVE, PRICE-SUBSIDIZED TRADE (May 2, 2012), *available at* http://www.americansolarmanufacturing.org/news-releases/05-02-12-chinas-five-year-plan.htm.
[1000] U.S. v. Wang Dong et al., 17 (W. D. Pa. May 1, 2014).
[1001] U.S. v. Wang Dong et al., 35 (W. D. Pa. May 1, 2014).
[1002] EU ProSun filed an anti-dumping complaint against certain photovoltaic products from China on July 25, 2012 with the European Commission. *See* European Commission, Notice of initiation of an anti-dumping proceeding concerning imports of crystalline silicon photovoltaic modules and key components (i.e. cells and wafers) originating in the People's Republic of China, 2012/C 269/04 (Sept. 9, 2012)
[1003] Fact Sheet, International Trade Administration, Department of Commerce, Commerce Finds Dumping and Subsidization of Crystalline Silicon Photovoltaic Cells, Whether or Not Assembled into Modules from the People's Republic of China (2012), *available at* http://ia.ita.doc.gov/download/factsheets/factsheet_prc-solar-cells-ad-cvd-finals-20121010.pdf.

> Commission,[1004] about one week before SolarWorld testified to the U.S. International Trade Commission about the harm caused by certain Chinese solar products,[1005] and two weeks before the U.S. Department of Commerce announced its final affirmative determination in its trade complaint against Chinese producers of solar cells.[1006]

As described more below in Part D, SolarWorld testified that these intrusions have resulted in significant harm to its business, including the loss of a competitive advantage and a loss of a return on its significant investment in a new solar technology.[1007]

b) U.S. Steel

According to the indictment, between February 8 and 23, 2010, 3PLA actors sent spearphishing e-mails with malware to U.S. Steel employees to gain unauthorized access to its network.[1008] On February 26, 2010, a 3PLA actor accessed at least one U.S. Steel computer and stole computer hostnames and descriptions for more than 1,700 U.S. Steel computers, including servers used for network security, applications for U.S. Steel employees' mobile devices, and physical access to U.S. Steel's facilities.[1009] The 3PLA actor then took steps to identify and exploit vulnerable servers on that list.[1010] In February 2010, at the same time as these cyber intrusions were occurring, U.S. Steel was a petitioner in two trade remedy investigations in the United States against imported steel products from China.[1011] The Chinese respondents named in these two

[1004] EU ProSun filed an anti-subsidies complaint against certain photovoltaic products from China on September 26, 2012 with the European Commission. *See* European Commission, *Notice of initiation of an anti-subsidy proceeding concerning imports of crystalline silicon photovoltaic modules and key components (i.e. cells and wafers), originating in the People's Republic of China*, 2012/C 340/06 (Nov. 8, 2012).

[1005] On October 3, 2012, the U.S. International Trade Commission held a hearing on the matter of certain photovoltaic products from China. *See* USITC, Inv. Nos. 701-TA-481 and 731-TA-1190, "Key Dates", *available at* https://www.usitc.gov/investigations/701731/2012/crystalline_silicon_photovoltaic_cells_and_modules/final.htm

[1006] On October 10, 2012, the U.S. Department of Commerce announced its affirmative final determinations in the antidumping and countervailing duty investigations of imports of certain photovoltaic cells from China. *See* Fact Sheet, INTERNATIONAL TRADE ADMINISTRATION, DEPARTMENT OF COMMERCE, *Commerce Finds Dumping and Subsidization of Crystalline Silicon Photovoltaic Cells, Whether or Not Assembled into Modules from the People's Republic of China* (2012).

[1007] Juergen Stein, SOLARWORLD AMERICAS INC. [*hereinafter* "SolarWorld"], *Testimony*, *Section 301 Hearing* 76 (Oct. 10, 2017).

[1008] U.S. v. Wang Dong et al., 20 (W. D. Pa. May 1, 2014). "In a spear-phishing attack, a target recipient is lured to either download a seemingly harmless file attachment or to click a link to a malware- or an exploit-laden site. The file, often a vulnerability exploit, installs a malware in a compromised computer. The malware then accesses a malicious command-and-control (C&C) server to await instructions from a remote user. At the same time, it usually drops a decoy document that will open when the malware or exploit runs to hide malicious activity." TREND MICRO INC., SPEAR-PHISHING EMAIL: MOST FAVORED APT ATTACK BAIT, RESEARCH PAPER 2012 (2012), *available at* http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-spear-phishing-email-most-favored-apt-attack-bait.pdf.

[1009] U.S. v. Wang Dong et al., 21 (W. D. Pa. May 1, 2014).

[1010] U.S. v. Wang Dong et al., 21 (W. D. Pa. May 1, 2014).

[1011] These two cases involved oil country tubular goods (OCTG), which are steel piping used by oil and gas companies and seamless standard line pipes (SSLP), which are steel pipes specifically constructed without a welded

investigations include the operating companies of several Chinese SOEs, including the Baosteel Group.[1012]

In U.S. Steel's submission to USTR in connection with this investigation, U.S. Steel explains that the second hack "resulted in the exfiltration of highly sensitive commercial secrets regarding [its] development of lightweight, high-strength steel."[1013] U.S. Steel responded by filing claims under Section 337 of the Trade Act before the U.S. International Trade Commission (USITC) against Baosteel, which it claims "was known to be one of the beneficiaries of China's state-sponsored cyber-attacks."[1014]

c) ATI

According to the indictment, on April 13, 2012, the 3PLA actors stole usernames and passwords for thousands of ATI employees.[1015] The stolen network credentials would have provided wide-ranging access to the company's computers and sensitive information.[1016] In 2012, ATI was engaged in a joint venture with Baosteel in Shanghai, which manufactures precision rolled stainless steel strips.[1017] On April 12, 2012, one day before the 3PLA exfiltrated these credentials, ATI officials met with officials from Baosteel in Shanghai for a board meeting[1018] related to their joint venture.

d) United Steel Workers (USW)

According to the indictment, the 3PLA stole sensitive information from USW computer networks on two separate occasions.[1019]

The indictment alleges that in January 2012, at the same time that USW was preparing a public campaign to counter what it viewed as a wide array of unfair Chinese government policies,

---

seam down the length of the pipes. *See* Department of Commerce, ITA Case No. A-570-943, A-570-956, and C-570-957.

[1012] Baosteel Group (now known as Baowu Steel) is a state-owned enterprise wholly-owned by China's State-owned Assets Supervision and Administration of Commission. *See* SASAC website for the full list, *available at* http://www.sasac.gov.cn/n2588035/n2641579/n2641645/index.html (last visited Jan. 23, 2018).

[1013] U.S. STEEL CORPORATION, *Submission, Section 301* Hearing (Sept. 28, 2017).

[1014] U.S. STEEL CORPORATION, *Submission, Section 301 Hearing* (Sept. 28, 2017).

[1015] U.S. v. Wang Dong et al., 22-3 (W. D. Pa. May 1, 2014).

[1016] U.S. v. Wang Dong et al., 21-3 (W. D. Pa. May 1, 2014).

[1017] *See Global Joint Ventures – Shanghai STAL Precision Stainless Steel Co., Ltd (STAL)*, ATI, *available at* https://www.atimetals.com/businesses/joint-ventures/Pages/default.aspx. *See also* Allegheny Technologies Incorporated, 2012 Form 10-K.

[1018] U.S. v. Wang Dong et al., 21-3 (W. D. Pa. May 1, 2014). Two months prior to this intrusion, the joint venture announced it was selling off its loss-making stainless steel assets to the Baosteel Group, its parent company for RMB 2.6 billion. The sale of assets to the Baosteel Group was the largest M&A transaction in China announced that month. See BAOSHAN IRON AND STEEL LTD. RELATED PARTY TRANSACTIONS REPORT. Report No. 2012-005, 24 (Feb. 29, 2012); See MIIT, MERGER AND RESTRUCTURING MONTHLY REPORT, VOL. 2, *available at* http://merger.miit.gov.cn/observation/briefing/2012-03-23/381.html.

[1019] U.S. v. Wang Dong et al., 7 (W. D. Pa. May 1, 2014).

V. Unauthorized Intrusions into U.S. Commercial Computer Networks and Cyber-Enabled Theft of Intellectual Property and Sensitive Commercial Information

3PLA stole sensitive information from USW computer networks.[1020] On January 31, 2012, USW issued a statement from its International President, calling on the U.S. Government to take action to protect the U.S. automobile and auto parts industry from "China's predatory, protectionist and illegal trade practices."[1021] USW through its trade counsel also released a report on Chinese auto policies that threaten the U.S. jobs in the auto industry on January 31, 2012.[1022] Meanwhile, on the same day, the 3PLA gained unauthorized access to USW computers, and stole e-mails from six senior USW employees, including USW's International President, most of whom were personally and publicly involved in formulating USW strategy towards combatting China's trade practices in this sector.[1023]

On March 7, 2012, 3PLA actors again gained unauthorized access to USW employees' e-mails[1024] at a critical period for USW as it was considering whether to request an extension of tariffs imposed on Chinese tires that would expire in September 2012.[1025] USW announced in September 2012 that it would not seek an extension of the tariffs, but revealed in its September announcement that it had notified the Administration in March that it would not seek an extension.[1026] The 3PLA stole e-mails from the inboxes of six senior employees that included sensitive, non-public, and deliberative information about USW trade strategy, including its decision not to seek an extension of the tariffs, which would not be announced publicly for another six months.[1027]

e) Westinghouse

Westinghouse was affected by four major cyber intrusions by the 3PLA – one occurring in May 2010, one in late December 2010, and two in early January 2011.[1028] According to the indictment, the PLA obtained at least 1.4 gigabytes of data, the equivalent of roughly 700,000 pages of e-mail messages and attachments from Westinghouse's computers,[1029] including: trade secrets; technical and design specifications; network credentials; and, sensitive e-mails belonging to senior decision-makers.[1030]

[1020] U.S. v. Wang Dong et al., 23 (W. D. Pa. May 1, 2014)
[1021] U.S. v. Wang Dong et al., 24 (W. D. Pa. May 1, 2014)
[1022] *See* Statement of Terence Stewart, Jan. 31, 2012 available at: http://assets.usw.org/releases/china-trade/Final-SS-Press-Release.pdf. See *also* LAW OFFICES OF STEWART & STEWART, CHINA'S SUPPORT PROGRAMS FOR AUTOMOBILES AND AUTO PARTS UNDER THE 12TH FIVE YEAR PLAN (Jan. 2012).
[1023] U.S. v. Wang Dong et al., 24-5 (W. D. Pa. May 1, 2014).
[1024] U.S. v. Wang Dong et al., 25 (W. D. Pa. May 1, 2014).
[1025] Imported Chinese tires became subject to a tariff for a period of three years starting on September 26, 2009, after the USW successfully petitioned the USITC for relief. *See Certain Passenger Vehicle and Light Truck Tires from the People's Republic of China*, Investigation No. TA-421-7, USITC Publication No. 4085.
[1026] USW announced on September 24, 2016 that it would not seek an extension of the tariffs. *USW Acclaim Success of Trade Relief for Tire Sector; Extension Not Requested*, UNITED STEELWORKERS (Sept. 24, 2012), available at: http://www.usw.org/news/media-center/releases/2012/usw-acclaim-success-of-trade-relief-for-tire-sector-extension-not-requested. The USW announcement states that it notified the Administration of its decision in March before the renewal request deadline
[1027] U.S. v. Wang Dong et al., 25-6 (W. D. Pa. May 1, 2014).
[1028] U.S. v. Wang Dong et al., 4, 15-6. (W. D. Pa. May 1, 2014).
[1029] U.S. v. Wang Dong et al., 16 (W. D. Pa. May 1, 2014).
[1030] U.S. v. Wang Dong et al., 2, 4, 15-6 (W. D. Pa. May 1, 2014).

V. Unauthorized Intrusions into U.S. Commercial Computer Networks and Cyber-Enabled Theft of Intellectual Property and Sensitive Commercial Information

In 2010, Westinghouse was building four AP1000 power plants in China and negotiating other terms of the construction, including technology transfers, with State Nuclear Power Technology Corporation (SNPTC), a Chinese SOE.[1031] At the same time, a 3PLA actor stole confidential and proprietary technical and design specifications for pipes, pipe supports, and pipe routing within the AP1000 plant buildings.[1032] The stolen trade secrets and technical information would permit a competitor to build a power plant without having to invest in associated research and development costs that had been borne by Westinghouse in the past.[1033]

Additionally, in 2010 and 2011, while Westinghouse was exploring other business ventures with SNPTC, a 3PLA actor stole sensitive, non-public, and deliberative e-mails belonging to senior decision-makers responsible for the Westinghouse business relationship with SNPTC.[1034] In January 2011, as the 3PLA were infiltrating Westinghouse's servers and exfiltrating its information, Westinghouse announced the signing of two agreements with SNPTC.[1035]

f) Alcoa

The indictment alleges that on February 1, 2008, Alcoa announced that it was entering into a partnership with a Chinese SOE, Chinalco to acquire an interest in a foreign mining company.[1036] After the announcement, on February 20, 2008, the 3PLA obtained access to nearly 3,000 Alcoa e-mails through a spearphishing message that installed malware into Alcoa's computer system.[1037] The stolen e-mails included internal discussions among Alcoa's senior managers regarding the acquisition of the foreign mining company.[1038]

The facts of each of these incidents provides a chilling warning to U.S. companies that engage or seek to engage in business in China or seek to challenge China's trade practices through legal means. If a company operates in a sector that China deems strategic to its economic interests or particularly if it has business relations with an SOE, the company must risk being targeted by Chinese government hackers for cyber intrusions and cyber theft, putting sensitive commercial information about its products, business strategy, and other matters at risk. These firms are forced to operate on the assumption that they are under constant surveillance by the Chinese

---

[1031] U.S. v. Wang Dong et al., 14 (W. D. Pa. May 1, 2014); *see also China signs first engineering contracts for Westinghouse AP1000-derived CAP1400 reactor*, POWER ENGINEERING, Nov. 29, 2010. *Foreign Companies Eyeing Chinese Nuclear Power Market*, SINOCAST, COMTEX NEWS NETWORK, Dec. 2, 2010; *First Concrete Pour for Haiyang Unit 2 Completed in Record Time; 4 AP1000 Units Now Under Construction in China*, PR NEWSWIRE, June 25, 2010.

[1032] U.S. v. Wang Dong et al., 14-5 (W. D. Pa. May 1, 2014).

[1033] U.S. v. Wang Dong et al., 14-5 (W. D. Pa. May 1, 2014).

[1034] U.S. v. Wang Dong et al., 16 (W. D. Pa. May 1, 2014)

[1035] *Westinghouse, China extend AP1000 reactor agreement*, POWER ENGINEERING, Jan. 20, 2011, *available at* http://www.power-eng.com/articles/2011/01/westinghouse--china.html.

[1036] U.S. v. Wang Dong et al., 26 (W. D. Pa. May 1, 2014); *see also* Eric Onstad, Lucy Hornby, *Chinalco and Alcoa buy stake in Rio Tinto*, NY TIMES (Feb. 1, 2008).

[1037] U.S. v. Wang Dong et al., 26-7 (W. D. Pa. May 1, 2014).

[1038] U.S. v. Wang Dong et al., 27 (W. D. Pa. May 1, 2014).

government's extensive system of corporate surveillance and control, which is discussed in greater detail in Section VI of this report.[1039]

3. China's Institutional Framework Supports Cyber Intrusions into U.S. Commercial Networks

As discussed in detail in other sections of this report, China relies primarily on a state-led approach to technology development and economic growth.[1040] Through an extensive planning system, China identifies certain sectors and technologies for development and fosters national champions to achieve dominance in both domestic and global markets.[1041] China's industrial plans and innovation goals, such as Made in China 2025,[1042] aim to provide support and assistance through the use of state resources to Chinese companies and commercial sectors.[1043] At the same time, China maintains an extensive state sector and uses state-invested enterprises and other mechanisms as instruments to achieve the government's economic objectives.

As noted above in Section IV.B.5, China's policy of "military-civil fusion" calls for the development of integrated information sharing platforms to facilitate science and technology (S&T) resource sharing and collaboration between state laboratories, the PLA, and enterprises.[1044] China's government-directed cyber capabilities exist alongside an institutional framework that provides state-invested enterprises and national champions with privileged access to various forms of Chinese government support and information.

Indeed, the U.S. government has evidence that the Chinese government provides competitive intelligence through cyber intrusions to Chinese state-owned enterprises through a process that includes a formal request and feedback loop, as well as a mechanism for information exchange via a classified communication system.

For example, according to U.S. government information, China National Offshore Oil Corporation (CNOOC), a state-owned enterprise, submitted formal requests to Chinese

---

[1039] Andrew Browne, *China's Big Brother Is Watching You Do Business*, WALL STREET J., May 23, 2017.
[1040] *See* Section I.C.
[1041] *See* Section I.C.
[1042] See Section I.C for more information on the Made in China 2025 policy.
[1043] For example, China's Made in China 2025 policy documents set out targets for developing ten key industries. U.S. CHAMBER OF COMMERCE, MADE IN CHINA 2025: GLOBAL AMBITIONS BUILT ON LOCAL PROTECTIONS 17-18 (2017) (stating that the policy "appears to provide preferential access to capital to domestic companies to promote their indigenous [research and development] capabilities, enhance their competitiveness, and support their ability to acquire technology from abroad."). U.S. CHAMBER OF COMMERCE, MADE IN CHINA 2025: GLOBAL AMBITIONS BUILT ON LOCAL PROTECTIONS 6 (2017) ("In concert with the 13th Five-Year Plan, Internet Plus Action Plan, and other state-led development plans, [Made in China 2025] constitutes a broader strategy to use state resources to alter and create comparative advantage in these sectors on a global scale."). EUROPEAN CHAMBER OF COMMERCE IN CHINA, CHINA MANUFACTURING 2025: PUTTING INDUSTRIAL POLICY AHEAD OF MARKET FORCES 1 (2017) (stating that the policy's references to "'indigenous innovation'—along with mentions of the need to realise 'self-sufficiency' . . . suggests that Chinese policies will further skew the competitive landscape in favour of domestic companies.").
[1044] *See Description of National New Industrial Demonstration Base*, MIIT, http://sfjd.miit.gov.cn/BaseInfoAction!findListIndustry.action

intelligence services seeking intelligence information on several U.S. oil and gas companies and on U.S. shale gas technology. One instance occurred in January 2012 in the context of commercial negotiations between a U.S. company ("U.S. Company 1"), CNOOC, and the PRC Ministry of Agriculture regarding oil leaks that had occurred at a facility jointly owned and operated by U.S. Company 1 and CNOOC in June 2011.

In January 2012, these Chinese intelligence services provided CNOOC information ahead of and during negotiations with U.S. Company 1. The information that the intelligence services provided to CNOOC included details on U.S. Company 1's position in the negotiation. CNOOC attributed their ultimate success in the negotiation with U.S. Company 1 to the information that CNOOC had received from the intelligence services. According to information the U.S. Government has access to, senior Chinese Intelligence officials, including a PLA director, Liu Xiaobei, endorsed the use of the intelligence information during CNOOC's negotiations with U.S. Company 1.

In a second instance, in July 2012, CNOOC requested that Chinese Intelligence provide specific information on five named U.S. oil and natural gas companies. Specifically, CNOOC sought information on:

> -U.S. Company 2's operations, asset management, and the movements of its senior personnel;
>
> -U.S. Company 3's developments in shale gas technology; and
>
> -The status of U.S. Company 4 and U.S. Company 5's research in certain areas, including lab procedures, fracking technology and fracking formulae.

These examples illustrate how China uses the intelligence resources at its disposal to further the commercial interests of Chinese state-owned enterprises to the detriment of their foreign partners and competitors.

Available evidence also indicates that China uses its cyber capabilities as an instrument to achieve its industrial policy and S&T objectives. Indeed, based on available information on China's cyber intrusions, experts have concluded that China's cyber intrusions and cyber theft align with its industrial policy goals.[1045] For example:

[1045] During the hearing for this investigation, Richard Ellings of the Commission on the Theft of American Intellectual Property and the President of the National Bureau of Asian Research, was asked whether there is a correlation between China's industrial plans and reported cyber intrusions directed against U.S businesses. Mr. Ellings testified in response: "Absolutely. In fact, the whole history of cyber intrusions and more broadly industrial espionage from China correlates with all the Five-year Plans, the Indigenous Innovation Policy that came out 10 years ago, 12 years ago, 11 years ago, current Five-year Plan, 2025 Plans. This is, as I said, kind of a standard that is given out to the country and to accomplish the goals set out in these plans becomes a measure by which cadres and entities throughout the country, their performance is measured. So they have tremendous incentive. So all of our tracking, whether they be through the court cases that make it into the public realm, whether cyber intrusion surveys and studies, Verizon did one, the Mandiant one, and so on, they all show a correlation between the priorities of the Chinese government at any time and the kinds of industrial espionage undertaken." Richard Ellings,

V. Unauthorized Intrusions into U.S. Commercial Computer Networks and Cyber-Enabled Theft of Intellectual Property and Sensitive Commercial Information

> As noted above, Mandiant observed in its 2013 report that "organizations in all industries related to China's strategic priorities are potential targets of APT1's comprehensive cyber espionage campaign." The victims of the intrusions in Mandiant's data set match industries that China has identified as strategic priorities in its five year plan and S&T development plans.[1046]
>
> In a review of cybertheft by a group associated with China's intelligence services, cybersecurity firm Novetta found the group targeting entities including Fortune 500 companies and firms with innovative information technology.[1047] Such targeting converged with China's strategic interests and the aims of China's 11th Five Year plan for the 2006-2011 period.[1048]
>
> In 2015, one cybersecurity expert testified to the U.S.-China Economic and Security Review Commission that "China's commercial cyber espionage activity likely supports Communist Party central planning policies designed to provide a competitive advantage for Chinese companies."[1049]

SolarWorld, in its submission to USTR, stated: "In our view, Chinese hacking and technology theft is pervasive and encouraged by the Chinese Government, as demonstrated by the 2014 indictment of the Chinese People's Liberation Army and as driven by China's Five Year Plans, which target specific high-tech and developing industries."[1050]

The 3PLA's cyber theft of trade secrets from Westinghouse, documented in the DOJ indictment, is illustrative of how China uses cyber theft as one of multiple instruments to achieve its state-led technology development goals. During China's 12th Five-year planning period (2011-2015), China issued several documents demonstrating its commitment to developing "indigenous" nuclear power technology capabilities. For example, the *12th Five-year Science and Technology Development Plan* expressly states that China should "comprehensively master" Westinghouse's AP1000 nuclear power design technology and "indigenously" complete standard designs at domestic facilities.[1051] The plan also states that China should establish demonstration power

---

COMMISSION ON THE THEFT OF AMERICAN INTELLECTUAL PROPERTY [*hereinafter* "IP Commission"], *Testimony*, *Section 301 Hearing* 51 (Oct. 10, 2017).

[1046] MANDIANT, APT1: EXPOSING ONE OF CHINA'S CYBER ESPIONAGE UNITS 24 (2013).

[1047] NOVETTA, OPERATION SMN: AXIOM THREAT ACTOR GROUP REPORT 4, 8-9 (2014). Such innovative technology includes telecommunications equipment manufacturers, infrastructure providers, integrated circuit manufacturers, software vendors, pharmaceutical and cloud computing companies, networking equipment manufacturers, and energy firms.

[1048] NOVETTA, OPERATION SMN: AXIOM THREAT ACTOR GROUP REPORT 9-10 (2014).

[1049] *Hearing on Commercial Cyber Espionage and Barriers to Digital Trade in China: Hearing Before the U.S.-China Econ. & Sec. Rev. Comm'n* (June 15, 2015) (Statement of Jen Weedon), *available* at https://www.uscc.gov/sites/default/files/Weedon%20Testimony.pdf; *see also* Richard J. Ellings, IP COMMISSION, *Submission*, *Section 301 Hearing* 3-4 (Sept. 28, 2017); *but see* James Lewis, CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES [*hereinafter* "CSIS"], *Submission, Section 301 Hearing* 4 (Sept. 2017).

[1050] SOLARWORLD, *Submission*, *Section 301 Hearing* 2 (Oct. 20, 2017).

[1051] *Notice on Issuing the 12th Five-year Science and Technology Development Plan (2011-2015)* § 3, Item 6 (MOST, Guo Ke Fa Ji [2011] No. 270, issued July 4, 2011).

plants for CAP1400 technology, which is China's domestic nuclear design technology based on Westinghouse's AP1000 design with its input.[1052] In addition, China's *12th Five-year Energy Technology Development Plan* contains specific references to developing the AP1000 and similar technologies through a process of "indigenization with outside support."[1053]

For Westinghouse to operate in China, Westinghouse was required to invest through a joint venture controlled by an SOE,[1054] SNPTC, and in order to win the bid it had to agree to transfer all relevant technology for the AP1000 to the SOE.[1055] This circumstance is hardly unique to Westinghouse. Section II of this report details how China uses its restrictive foreign investment regime to put pressure on U.S. companies to transfer technology to Chinese enterprises, often state-owned enterprises. As described above, according to the DOJ indictment, 3PLA actors stole thousands of files from Westinghouse's computers, including: trade secrets; technical and design specifications; network credentials; and sensitive e-mails belonging to senior decision-makers, while commercial negotiations between Westinghouse and SNPTC were ongoing.[1056]
In sum, China first expressly identified through its industrial policies a U.S. technology that China sought to indigenize. China then required technology transfer to an SOE in order for the U.S. company holding the technology to be able to access the China market. China then used its cyber capabilities to steal commercially sensitive information, including trade secrets, negotiating positions and technical designs, from the U.S. company that could provide the SOE with an advantage in its business dealings with the U.S. company.

4. China's Recent Cyber Intrusion Activities Against U.S. Commercial Networks

Beginning in 2014, the United States began stepping up pressure on China for its cyber intrusions into U.S. firms and the theft of commercial information through a number of mechanisms. In September 2015, then-U.S. President Obama and Chinese President Xi reached a commitment that "neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial

[1052] *Notice on Issuing the 12th Five-year Science and Technology Development Plan (2011-2015)* § 3, Item 6 (MOST, Guo Ke Fa Ji [2011] No. 270, issued July 4, 2011).
[1053] *12th Five-year Plan for Energy Technology (2011-2015)*, § 2.2, § 4.3 (NEA, issued Dec. 2011).
[1054] See e.g., *Catalogue of Industries for Guiding Foreign Investment*, (2007 Amendment) (NDRC, MOC Order No. 57, issued Oct. 31, 2007) , Part IV, para. 4 "Catalogue of Restricted Industries for Foreign Investment."
[1055] *Westinghouse Wins Nuclear Power Bid*, CHINA DAILY, Dec. 27, 2006 ("According to the [chief representative of Westinghouse China], the company's success can be mainly attributed to three factors: advanced technology, competitive pricing and an offering of all-round technology transfer… [The CEO of] Westinghouse, earlier told China Daily that Westinghouse will fully co-operate with its Chinese customers to transfer all technology as requested"); *See Foreign Companies Eyeing Chinese Nuclear Power Market*, SINOCAST, COMTEX NEWS NETWORK, Dec. 2, 2010 (Westinghouse delivered "more than 75,000 pieces of documents to Chinese customers as part of a technology transfer agreement, hoping to consolidate its leading status in the world's largest nuclear power market. The World Nuclear Association (WNA) believes that it is just because Westinghouse Electric agrees to transfer technology in its contracts with Chinese customers that it successfully wins the bid to build AP1000 nuclear reactors in China.").
[1056] U.S. v. Wang Dong et al. at 4.

sectors."[1057] The United States has been closely monitoring China's cyber activities since this consensus was reached, and the evidence indicates that cyber intrusions into U.S. commercial networks in line with Chinese industrial policy goals continue.

Beijing's cyber espionage against U.S. companies persists and continues to evolve. The U.S. Intelligence Community judges that Chinese state-sponsored cyber operators continue to support Beijing's strategic development goals, including its S&T advancement, military modernization, and economic development.

In September 2017, the DOJ filed an indictment against three Chinese nationals who "were owners, employees and associates of the Guangzhou Bo Yu Information Technology Company Limited[1058] (Boyusec), a company that cybersecurity firms have linked to the Chinese government.[1059] Three firms, all with operations in the United States, are named in the indictment as victims: Moody's Analytics, Siemens AG, and Trimble Inc. The cyber intrusions against Trimble continued until March 2016 (and the related conspiracy which continued until "at least May 2017"[1060]), targeted the three named firms to steal confidential business and commercial information and work product.[1061]

Specifically, in 2015 and 2016, Trimble was working to develop a new global navigation satellite systems product that "combined software with a relatively low cost antenna to significantly improve the positioning accuracy of mobile devices"[1062] (Commercial GNSS Project). "Beginning no later than December 2015, and continuing through March 2016, the co-conspirators targeted the servers within Trimble's network," and by the middle of January 2016 the hackers had "accessed Trimble's network and copied, packaged, and stole computer files containing commercial business documents and data" related to the GNSS project."[1063] In addition to the theft of market research and strategy information, the stolen files also included

[1057] Press Release, The White House, Fact Sheet: President Xi Jinping's State Visit to the United States (Sept. 25, 2015), https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states. DOJ reaffirmed the 2015 joint statement in October 2017: "Both sides will continue their implementation of the consensus reached by the Chinese and American Presidents in 2015 on U.S.-China cybersecurity cooperation… [including] (2)that neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantage to companies or commercial sectors[.]" *See* Press Release, First U.S.-China Law Enforcement and Cybersecurity Dialogue (Oct. 6, 2017), *available at* https://www.justice.gov/opa/pr/first-us-china-law-enforcement-and-cybersecurity-dialogue.

[1058] U.S. v. Wu Yingzhou et al., (September 13, 2017) (Crim. No. 17-247 W.D.Pa.).

[1059] There have been many public reports linking the firm Boyusec with China's Ministry of State Security (MSS) and/or the PLA's cyber unit. For example, a report from a private cybersecurity firm, Recorded Future, published on May 17th, 2017, links Boyusec to the Chinese Ministry of State Security. The report alleges that the known threat actor group "APT3" is in fact Boyusec and is directly linked to the Chinese state. Insikt Group, *Recorded Future Research Concludes Chinese Ministry of State Security Behind APT3,* RECORDED FUTURE, May 17, 2017 (linking these attacks to the MSS). *See also Siemens, Trimble, Moody's breached by Chinese Hackers, U.S. Charges,* REUTERS, Nov. 27, 2017 (linking Boyusec hacks to the PLA).

[1060] U.S. v. Wu Yingzhou et al., at 3.

[1061] U.S. v. Wu Yingzhou et al., at 3-9.

[1062] U.S. v. Wu Yingzhou et al., at 7.

[1063] U.S. v. Wu Yingzhou et al., at 8.

"confidential and proprietary schematic design for the hardware receiver equipment"[1064] and "two directory lists […] listed files containing the names of a Trimble engineer related to the Commercial GNSS Project."[1065] "In total, conspirators stole at least 275 megabytes of data, including compressed data, which included hundreds of files that would have assisted a Trimble competitor in developing, providing, and marketing similar software and subscriptions services, without incurring millions of dollars in research and development costs."[1066] According to the indictment, intended customers of the Commercial GNSS Project included construction, land survey, and agricultural sectors and the technology had no military applications.[1067]

Similarly, U.S. cybersecurity firms have concluded that cyber intrusions against U.S. firms by Chinese state-sponsored and supported hackers since September 2015 have decreased or become more difficult to detect, but none has concluded that the activity has ceased entirely.[1068] In June 2016, the cybersecurity firm FireEye[1069] stated in a report that while cyber intrusions appear to be less voluminous, the attacks appear to now be more focused.[1070] According to the report, FireEye observed 262 cyber intrusions from late 2015 through mid-2016, conducted by 72 different China-based groups whose identities range from "government and military actors, contractors, patriotic hackers, and even criminal elements."[1071] Of the 262 observed intrusions, 182 involved the networks of private and public U.S. entities.[1072] FireEye recorded that in April and May 2016, "three groups compromised the networks of four firms headquartered in the United States, Europe, and Asia that are involved in the manufacturing of semiconductors and chemical components used in the production of semiconductors."[1073]

One of the more notable exceptions to the observed decline comes from APT10, which is believed by several cybersecurity firms to be a Chinese cyber espionage group.[1074] In late 2016, BAE Systems and PricewaterhouseCoopers reported that they had been investigating a campaign of

[1064] U.S. v. Wu Yingzhou et al., at 8.
[1065] U.S. v. Wu Yingzhou et al., at 9.
[1066] U.S. v. Wu Yingzhou et al., at 9.
[1067] U.S. v. Wu Yingzhou et al., at 7.
[1068] FIREEYE, REDLINE DRAWN: CHINA RECALCULATES ITS USE OF CYBER ESPIONAGE 12-14 (2016).
[1069] FireEye is now the parent company of Mandiant.
[1070] Robert Hackett, *China's Cyber Spying on the U.S. Has Drastically Changed*, FORTUNE, June 25, 2016, (interviewing Laura Galante of FireEye). *See also* FIREEYE, REDLINE DRAWN: CHINA RECALCULATES ITS USE OF CYBER ESPIONAGE 4 (2016). FireEye concludes that Chinese cyberintrusions and cybertheft were decreasing since mid-2014 due to a number of factors including "ongoing [Chinese] military reforms, widespread exposure of Chinese cyber operations, and actions taken by the U.S. government." *Id.* at 4; *see also* IP COMMISSION, UPDATE TO THE IP COMMISSION REPORT (2017) ("cyberattacks may have declined in volume since about 2014, although whether this is a result of a crackdown in China on responsible units in the People's Liberation Army (PLA) or other factors is not entirely clear."). Other commenters note the decrease in activity linking it to the September 2015 joint statement as well as ongoing Chinese PLA reorganization, see, for example, James Lewis, CSIS, *Submission, Section 301 Hearing* 5 (Sept. 2017); and Erin Ennis, U.S.-CHINA BUSINESS COUNCIL [*hereinafter* "USCBC"], *Testimony*, *Section 301 Hearing* (Oct. 10, 2017) (referring to FireEye's June 2016 report concluding "a notable decrease in reports by American companies of intrusions from suspected Chinese hackers.").
[1071] FIREEYE, REDLINE DRAWN: CHINA RECALCULATES ITS USE OF CYBER ESPIONAGE 15 (2016).
[1072] FIREEYE, REDLINE DRAWN: CHINA RECALCULATES ITS USE OF CYBER ESPIONAGE 12 (2016).
[1073] FIREEYE, REDLINE DRAWN: CHINA RECALCULATES ITS USE OF CYBER ESPIONAGE 13 (2016).
[1074] *See e.g.*, FireEye, APT10 (MenuPass Group): New Tools, Global Campaign Latest Manifestation of Longstanding Threat (Apr. 6, 2017); *See also* BAE Systems, *APT10 – Operation Cloud Hopper*, (2017).

intrusions, referred to as "Operation Cloud Hopper" by APT10 against several major IT managed service providers, including some U.S. companies.[1075] According to BAE, APT10's targeting is consistent with "industries that align with China's 13th Five-year Plan which would provide valuable information to advance the domestic innovation goals held within China."[1076] FireEye believes that APT10's activities historically have been "in support of Chinese national security goals, including acquiring valuable military and intelligence information as well as the theft of confidential business data to support Chinese corporations."[1077]

BAE notes that APT10's activities use a strategy that is difficult to trace.[1078] By targeting IT managed service providers, APT10 is seeking the ability "to move laterally onto the networks of potentially thousands of other victims" and "has been observed to exfiltrate stolen intellectual property" while evading a network's defenses.[1079] BAE concludes that APT10 has increased its sophistication and has "significant staffing and logistical resources, which have increased over the last three years, with a significant step-change in 2016."[1080]

Another cybersecurity firm, Fidelis Cybersecurity, concluded that APT10 installed malware on the website of the National Foreign Trade Council (NFTC), such that when U.S. member companies registered for NFTC's board meeting scheduled for March 2017, the malware would be executed on their computers.[1081] According to Fidelis Cybersecurity, this particular malware would allow APT10 to exploit vulnerabilities known to exist within the user's applications.[1082] NFTC board members that may have sought to register for the meeting include a large group of leading U.S. companies across a wide range of commercial sectors.[1083]

[1075] PWC, BAE SYSTEMS, APT10 – OPERATION CLOUD HOPPER (2017), *available at* https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-report-final-v4.pdf.
[1076] PWC, BAE SYSTEMS, APT10 – OPERATION CLOUD HOPPER 15 (Apr. 2017).
[1077] *APT10 (MenuPass Group): New Tools, Global Campaign Latest Manifestation of Longstanding Threat*, FIREEYE, Apr. 6, 2017, https://www.fireeye.com/blog/threat-research/2017/04/apt10_menupass_grou.html.
[1078] PWC, BAE SYSTEMS, APT10 – OPERATION CLOUD HOPPER (Apr. 2017).
[1079] PWC, BAE SYSTEMS, APT10 – OPERATION CLOUD HOPPER 8 (Apr. 2017).
[1080] PWC, BAE SYSTEMS, APT10 – OPERATION CLOUD HOPPER 5 (Apr. 2017). FireEye, in April of 2017 agreed that APT10 had expanded their operations. *See APT10 (MenuPass Group): New Tools, Global Campaign Latest Manifestation of Longstanding Threat*, FIREEYE, Apr. 6, 2017.
[1081] *Operation TradeSecret: Cyber Espionage at the Heart of Global Trade*, FIDELIS CYBERSECURITY (Apr. 6, 2017), https://www.fidelissecurity.com/TradeSecret.
[1082] *Operation TradeSecret: Cyber Espionage at the Heart of Global Trade*, FIDELIS CYBERSECURITY (Apr. 6, 2017).
[1083] According to NFTC's website, board members include: ABB Incorporated, Amazon, Amgen, Applied Materials, Baxter International, British American Tobacco, Caterpillar Incorporated, Chevron, Cisco Systems, Inc., The Coca-Cola Company, ConocoPhillips, Inc, Corning Incorporated, Deloitte & Touche, LLP, Dentons US LLP, DHL Express (USA) Inc., E.I. du Pont de Nemours & Company, eBay Inc., Ernst & Young LLP, ExxonMobil Corporation, FCA US LLC, FedEx Express, Fluor Corporation, Ford Motor Company, General Electric Company, Google Inc., Halliburton Company, Hanesbrands Inc., Hewlett Packard Enterprise Company, HP Inc, IBM Corporation, Johnson Controls, KPMG, LLP, Mars Incorporated, Mayer Brown LLP, McCormick & Company, Inc., Microsoft Corporation, Mondelēz International, Occidental Petroleum Corporation, Oracle Corporation, Pernod Ricard USA, Pfizer Inc., PMI Global Services Inc, PricewaterhouseCoopers LLP, Procter & Gamble Company, Qualcomm Incorporated, Siemens Corporation, TE Connectivity, Toyota Motor Sales, USA, Incorporated, United Technologies Corporation, UPS, Visa Inc, and Wal-mart Stores.

V. Unauthorized Intrusions into U.S. Commercial Computer Networks and Cyber-Enabled Theft of Intellectual Property and Sensitive Commercial Information

The data set since September 2015 is necessarily more limited than the extensive data collected over the last decade on Chinese cyber intrusions and cyber theft. Notwithstanding an apparent decline in the observed number of cyber incidents, the continued use of cyber intrusions by the Chinese government targeting U.S. companies remains a serious problem. State-sponsored cyber intrusions originating from China into U.S. commercial networks occur alongside China's institutional framework for promoting its industrial and technological development through a state-led model in which state-owned enterprises and national champions are the recipients of extensive state support. In sum, the evidence indicates that China continues its policy and practice, spanning more than a decade, of conducting and supporting cyber-enabled theft and intrusions into the commercial networks of U.S. companies. This conduct provides the Chinese government with unauthorized access to intellectual property, trade secrets, or confidential business information, including, but not limited to, technical data, negotiating positions, and sensitive and proprietary internal business communications. Indeed, the U.S. Chamber of Commerce in its submission states that the "U.S. industry does not believe there has been a full cessation of cyber enabled IP theft, and we urge the Trump Administration to ensure the Chinese government upholds the agreement."[1084]

C. China's Acts, Policies, and Practices Regarding Cybertheft of Intellectual Property Are Unreasonable

As described above, the statute defines an "unreasonable" act, policy, or practice as one that "while not necessarily in violation of, or inconsistent with, the international legal rights of the United States is otherwise unfair and inequitable."[1085] The statute expressly provides that acts, policies, or practices that are unreasonable includes those that deny fair and equitable provision of "adequate and effective protection of intellectual property rights notwithstanding the fact that the foreign country may be in compliance with the specific obligations of the Agreement on Trade-Related Aspects of Intellectual Property Rights."[1086]

It is the longstanding policy of the United States, most recently reaffirmed in 2014 in Presidential Policy Directive 28 (PPD-28), that "[t]he collection of foreign private commercial information or trade secrets is authorized only to protect the national security of the United States or its partners and allies. It is not an authorized foreign intelligence or counterintelligence purpose to collect such information to afford a competitive advantage to U.S. companies or U.S. business sectors commercially."[1087]

In fact, China's activities stand in contrast to domestic and international standards adopted around the world. Many countries prohibit and even criminalize the unauthorized intrusions into computer networks in certain circumstances, including intrusions that result in

[1084] U.S. CHAMBER OF COMMERCE, *Submission*, *Section 301 Hearing* 38 (Oct. 3, 2017).
[1085] 19 U.S.C. § 2411(d)(3)(A).
[1086] 19 U.S.C. § 2411(d)(3)(B)(i)(II).
[1087] *Presidential Policy Directive – 2014 Directive on Signals Intelligence Activities*, Daily Comp. Pres. Docs. Section 1(c) (Jan. 17th, 2014), https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

misappropriation of trade secrets.[1088] Moreover, countries around the world have repeatedly condemned activities by government actors to misappropriate trade secrets for commercial purposes. For example, leaders of the 21-member Asia-Pacific Economic Cooperation (APEC), which includes China, in November 2016 "reaffirm[ed] that economies should not conduct or support information and communications technology (ICT)-enabled theft of intellectual property or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors."[1089] Similarly, in November 2015, at the Antalya Summit, the G20 Leaders' Communique stated: "In the ICT environment, just as elsewhere, states have a special responsibility to promote security, stability, and economic ties with other nations. In support of that objective, we affirm that no country should conduct or support ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors."[1090]

The fact that a wide group of countries, including China have condemned ICT-enabled theft of intellectual property by foreign governments reinforces the conclusion that government acts, policies, and practices involving cyber theft of trade secrets for a commercial purpose is unreasonable.

Claims that there is no meaningful distinction between the Chinese government's cyber activities and that of other countries, including the United States, are not valid. China's cyber intrusions are unique from those of Western market economies because the intrusions occur within the framework of China's extensive state-driven economic development model, which has no parallel in Western market economies. Not only does the United States not rely on extensive industrial policy tools to identify specific commercial sectors and commercial technologies for development, the United States does not have national champions and state-

[1088] *See e.g.*, In the UK, Computer Misuse Act, 1990, § 1(1)(a); in Ireland, Criminal Damage Act, 1991, § 5(1); in Sweden, Lag (1990:409) Protection of Business Secrets Act and Brottsbalken [BrB][Criminal Code] 4:9c (Swed); in Italy, C.p. 615.ter; in Germany, Strafgesetzbuch [STGB][Penal Code] S (202)(2) and (303)(b); in Japan, [Unauthorized Computer Access Act], Law No. 128 of 1999, art. 3(2).

[1089] *Fact Sheet: 24th Annual APEC Economic Leaders' Meeting*, White House Office of the Press Secretary (Nov. 20, 2016), *available at* https://obamawhitehouse.archives.gov/the-press-office/2016/11/20/fact-sheet-24th-annual-apec-economic-leaders-meeting. In addition, the APEC leaders adopted a series of best practices on trade secret protection and enforcement against misappropriation that recognizes that APEC economies should consider applying criminal liability for the willful theft of trade secrets that can arise through electronic intrusions for a commercial advantage. *See* https://ustr.gov/sites/default/files/11202016-US-Best-Practices-Trade-Secrets.pdf.

[1090] G20 LEADERS' COMMUNIQUE, ANTALYA SUMMIT ¶26 (Nov. 2015), *available at* http://g20.org.tr/g20-leaders-commenced-the-antalya-summit/. In September 2017, the G7 issued the following G7 ICT and Industry Ministers' Declaration, "reaffirm[ing] that no country should conduct or support ICT-enabled infringement or misappropriation of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors." G7 ICT and Industry Ministers' Declaration Making the Next Production Revolution Inclusive, Open and Secure (Sept. 26 2017).

owned enterprises to implement such policies. In other words, U.S. companies "do not have the advantage of leveraging government intelligence data for commercial gain."[1091]

Moreover, China's troubling track record of using cyber intrusion and cyber theft to target U.S. companies in sectors prioritized by China's industrial policies is "hurting the case for free trade" because "[m]utually beneficial economic exchange occurs only when there is acceptance of the rule of law. If the legal protection of property rights is ignored, free exchange makes much less sense: One side just takes from the other."[1092]

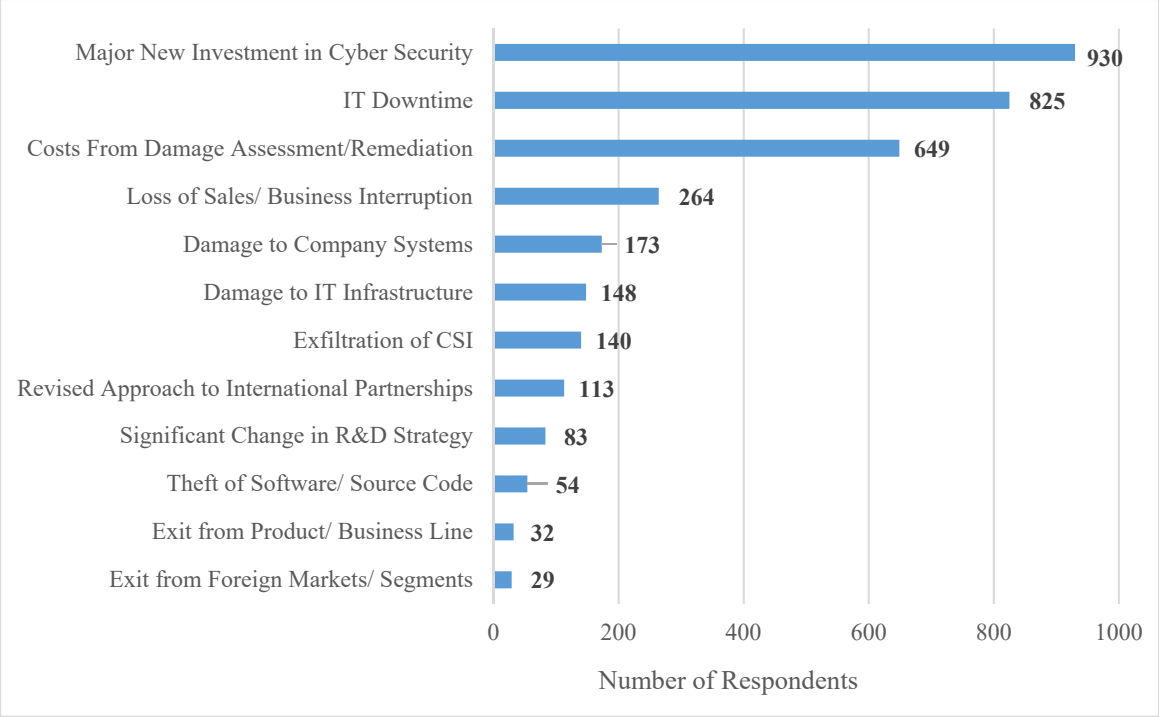
Based on the foregoing factors, China's acts, policies, and practices of cyber intrusions into the computer networks of U.S. business and the theft of firms' sensitive commercial information are unreasonable.

D. China's Acts, Policies, and Practices Regarding Cybertheft of Intellectual Property Burden U.S. Commerce

China's cyber intrusion and cyber theft activities harm U.S. business interests in a variety of ways. It can be difficult to assess the full burden on U.S. commerce because of chronic under reporting, companies being unaware that their network have been compromised or being unaware of the extent of the damage done. Nevertheless, a recent survey conducted by the Bureau of Industry and Security (BIS) contains the responses of more than 8,000 companies in the United States about the impact they face from malicious cyber activity from all sources. Respondents noted the following impacts in descending order:

[1091] *Cyber Espionage and the Theft of U.S. Intellectual Property and Technology: Hearing Before the House of Representatives Committee on Energy and Commerce Subcommittee on Oversight and Investigations* (July 9, 2013) (statement of Larry M. Wortzel).
[1092] Derek Scissors, *Chinese Economic Espionage Is Hurting the Case for Free Trade*, HERITAGE (Nov. 19, 2012), http://www.heritage.org/trade/report/chinese-economic-espionage-hurting-the-case-free-trade.

V. Unauthorized Intrusions into U.S. Commercial Computer Networks and Cyber-Enabled Theft of Intellectual Property and Sensitive Commercial Information



Source: U.S. Department of Commerce, Bureau of Industry and Security, Ongoing Defense Industrial Base Assessment.

First and foremost, cyber intrusions and cyber theft damage company performance and competitiveness, and result in lost sales, lost revenue, disruption of supply chains, lost business opportunities, and failure to achieve return on investment. For example, SolarWorld in its submission to USTR in connection with this investigation stated that the Chinese government's cyber-theft of its proprietary business information "resulted in more than $120 million in damages in the form of lost sales and revenue" because Chinese producers entered the market earlier than expected based on the proprietary information taken.[1093] SolarWorld's statement also provided the following:

> The injury to SolarWorld and other solar manufacturers is particularly acute, given the [Chinese] government subsidized Chinese producers of solar cells and panels, who appear to have benefited from the stolen trade secrets, have been flooding the U.S. marked with dumped products, since 2012, driving nearly 30 U.S. companies out of business, and leaving the U.S. solar manufacturing industry on the brink of collapse.[1094]

At the hearing, Solar World America's CEO, Jürgen Stein, testified:

[1093] SOLARWORLD, *Submission*, *Section 301 Hearing* 3-6 (Oct. 20, 2017) ("SolarWorld strongly believes that this [early entry of Chinese solar competitors] was the result of information stolen from SolarWorld's systems and provided to SolarWorld's Chinese competitors.").
[1094] SOLARWORLD. *Submission*, *Section 301 Hearing* 5-6 (Sept. 28, 2017).

V. Unauthorized Intrusions into U.S. Commercial Computer Networks and Cyber-Enabled Theft of Intellectual Property and Sensitive Commercial Information

> [SolarWorld's] efforts to stay ahead of the Chinese wave of illegally dumped and subsidized lower power and quality imports were thwarted by the hacking and theft of proprietary information about the [passivated emitter rear contact (PERC)] process that we had innovated. Between May and September 2012, exactly the time we brought this technology to mass production, SolarWorld's IT system was hacked 13 times by Chinese military hackers. Now, armed with our proprietary data and armed with our cost data, we saw our Chinese competitors leap overnight into PERC technology that we had innovated and with economic information that would unfairly enhance their positions in price negotiations.
>
> By early 2014, a prominent Chinese-based solar rival, JA Solar, announced it was converting to PERC technology, and it began mass production of PERC in May of that year.[1095] By early 2015, Chinese-based Trina announced its own PERC conversion and came to the market later that year with a comparable PERC technology.
> While the five Chinese military hackers have never been brought to justice in this country, we firmly believe that were it not for their economic espionage and theft from SolarWorld Americas, Chinese solar producers like JA Solar and Trina would have taken far longer to make the leap into PERC technology. State-sponsored hacking and theft by China greatly weakened SolarWorld's first-mover status and again left SolarWorld vulnerable to China's relentless effort to take over the U.S. solar industry through the sale of solar cells and panels below the cost of production.[1096]

In a post-hearing submission to USTR, SolarWorld stated:

> Perhaps the greatest loss that SolarWorld has sustained, and continues to sustain, as a result of the Chinese government's cyberhacking is the unfair loss of its competitive advantage, thereby resulting in significant losses in market leadership, sales, and profitability.... SolarWorld has invested in significant R&D and in the application of new technologies in its manufacturing process, all with the goal of moving solar technology forward and successfully competing with the unfairly-priced solar cell and module imports from manufacturers in Asia. These efforts, however, were lost almost overnight when Chinese state-backed actors infiltrated SolarWorld's systems and stole its proprietary information. This loss has been devastating to SolarWorld. As explained in [SolarWorld CEO's] testimony, SolarWorld worked for eight years on the development of the state-of-the-art Passivated Emitter Rear Contact (PERC) technology.' After years of R&D, SolarWorld became the first manufacturer to industrialize PERC cell production, an advantage, based on the price premium for the state-of-the-art technology and high-quality materials used to produce quality product, that we expected to remain for several years. Instead, SolarWorld's significant investments in this technology - estimated at approximately $60 million in R&D and $600 million total in setting up all

[1095] In its post-hearing submission, SolarWorld provided a correction that JA Solar announced it had launched its PERC product in October 2013. SOLARWORLD, *Submission*, *Section 301 Hearing* 5 (Oct. 20, 2017).
[1096] Juergen Stein, SOLARWORLD, *Testimony*, *Section 301 Hearing* 76 (Oct. 10, 2017).

production sites, equipment and processes – have been undercut by Chinese competitors.[1097]

As the SolarWorld example illustrates, Chinese cyber theft of commercially sensitive information often takes place in industries that the Chinese government has prioritized for state-support, and the victims often operate in U.S. industries that are already suffering from the result of China's other policy tools.

Moreover, U.S. companies often lack effective recourse under U.S. or Chinese law after they have been a victim of a Chinese cyber intrusion or cyber theft to recover the damages they incurred from such activity. As described above, the practical and financial challenges of litigation prevented U.S. Steel from being able to seek legal relief against its well-funded Chinese SOE adversary in litigation.[1098]

In addition, there are significant remediation costs a company must incur after a cyber intrusion. Even if the hackers are ultimately unable to monetize all the information they have stolen, the victim must expend significant resources to deal with the potential implications. Cyber intrusions and cybertheft can lead to service disruptions that interrupt a firm's sales or other operations.[1099] According to one study, it takes on average 191 days to identify that a data breach has occurred, and 66 days to contain it.[1100] Containing a data breach requires "forensic and investigative activities, assessment and audit services, crisis team management and communications to executive management and board of directors."[1101]

Even after a data breach is contained, companies bear significant additional burdens including "legal expenditures . . . identity protection services and regulatory interventions."[1102] Reputational damage is also a burden that companies in many instances bear after experiencing cyber intrusion or cyber theft. After such breaches, experts observe that a company's valuation may decrease from a drop in stock prices after the company publicly reports that it has been hacked.[1103]

At the macro-level, one study concluded that cyber intrusions and cyber theft have a significant impact on U.S. employment. A report by the Center for Strategic and International Studies

[1097] SOLARWORLD, *Submission*, *Section 301 Hearing* 2-4 (Oct. 20, 2017).
[1098] U.S. STEEL, *Submission*, *Section 301 Hearing* 2 (Sept. 28, 2017).
[1099] MCAFEE, CSIS, THE ECONOMIC IMPACT OF CYBERCRIME AND CYBER ESPIONAGE 10 (July 2013).
[1100] PONEMON INSTITUTE, 2017 COST OF DATA BREACH STUDY 3 (June 2017).
[1101] PONEMON INSTITUTE, 2017 COST OF DATA BREACH STUDY 3 (June 2017). The report details these activities further: "Conducting investigations and forensics to determine the root cause of the data breach; Determining the probable victims of the data breach; Organizing the incident response team; Conducting communication and public relations outreach; Preparing notice documents and other required disclosures to data breach victims and regulators; Implementing call center procedures and specialized training." *Id*. at 29.
[1102] PONEMON INSTITUTE, 2017 COST OF DATA BREACH STUDY 3 (June 2017).
[1103] MCAFEE, CSIS, THE ECONOMIC IMPACT OF CYBERCRIME AND CYBER ESPIONAGE at 12-13. The report notes that valuation drops typically do not appear to be permanent; however, financial transactions and lost expectations occurring during the window of any valuation drop would reasonably have an impact on the firm.

(CSIS) and McAfee, found that cybercrime from all sources costs approximately 200,000 jobs annually in the United States.[1104] According to CSIS, "Cybercrime is a tax on innovation and slows the pace of global innovation by reducing the rate of return to innovators and investors…For developed countries; cybercrime has serious implications for employment. The effect of cybercrime is to shift employment away from jobs that create the most value. Even small changes in GDP can affect employment."[1105]

For all of the foregoing reasons, China's cyber activities targeting U.S. companies poses significant costs on U.S. companies and burdens U.S. commerce.

[1104] Press Release, McAfee and CSIS: Stopping Cybercrime Can Positively Impact World Economies (June 9, 2014), https://www.mcafee.com/us/about/news/2014/q2/20140609-01.aspx.
[1105] Press Release, McAfee and CSIS: Stopping Cybercrime Can Positively Impact World Economies (June 9, 2014), https://www.mcafee.com/us/about/news/2014/q2/20140609-01.aspx.