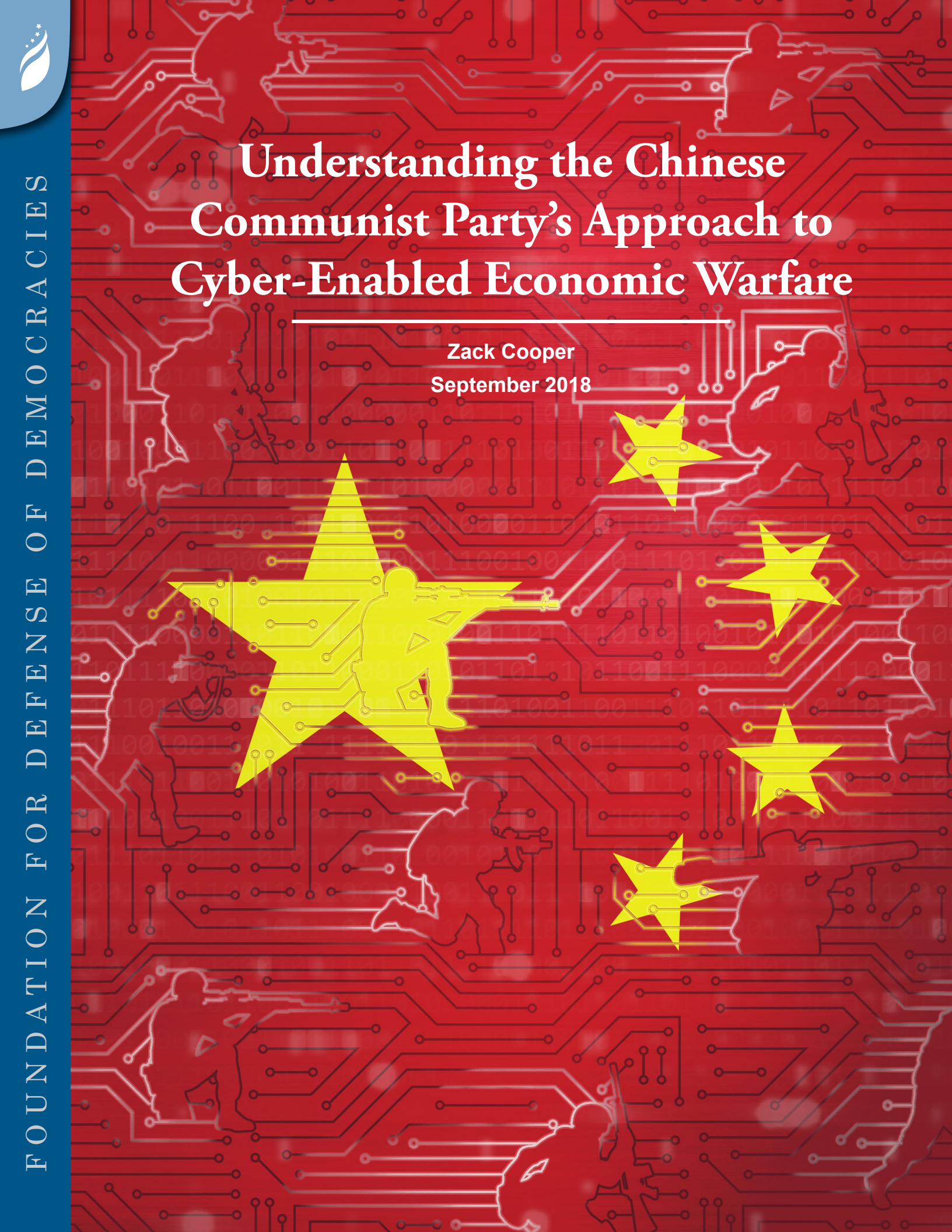

FOUNDATION FOR DEFENSE OF DEMOCRACIES

Understanding the Chinese Communist Party's Approach to Cyber-Enabled Economic Warfare

Zack Cooper

September 2018

Understanding the Chinese Communist Party's Approach to Cyber-Enabled Economic Warfare

Zack Cooper

September 2018

FDD PRESS

A division of the
FOUNDATION FOR DEFENSE OF DEMOCRACIES
Washington, DC

Table of Contents

Executive Summary

American prosperity and security are challenged by an economic competition playing out in a broader strategic context … Every year, competitors such as China steal U.S. intellectual property valued at hundreds of billions of dollars. Stealing proprietary technology and early-stage ideas allows competitors to unfairly tap into the innovation of free societies. Over the years, rivals have used sophisticated means to weaken our businesses and our economy as facets of cyber-enabled economic warfare.

- U.S. National Security Strategy (2017)[1]

The United States and the People's Republic of China (PRC) are engaged in an increasingly intense political, economic, and military competition spanning not only throughout East Asia, but also around the globe. In this competition, China uses cyber means to enhance its strategic position vis-à-vis the United States and its allies and partners. China is engaged in wide-ranging cyber intrusions and network exploitations causing massive damage to U.S. and other foreign firms annually.[2] By advantaging Chinese enterprises at the expense of competitors from the United States and its allies and partners, these attacks cumulatively degrade U.S. national security. This cyber campaign is an integral part of China's broader security strategy and has undermined both American prosperity and security. And yet, it has not garnered the public attention warranted by its severity.[3]

For years, the Chinese government has engaged in cyber-enabled economic espionage[4] and other covert and clandestine activities to strengthen China's economic competitiveness and strategic position.[5] China is estimated to be responsible for 50 to 80 percent of cross-border intellectual property theft worldwide,[6] and over 90 percent of cyber-enabled economic espionage in the United States.[7] Various study groups have estimated that Chinese intellectual

1. The White House, "National Security Strategy of the United States of America," December 2017. (https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf)

2. Although this report uses the term "cyber," Chinese literature typically refers to either "information security" or "network security."

3. Notable reports on Chinese cyber-enabled economic espionage include: Dennis C. Blair and Jon M. Huntsman, Jr., "The Theft of American Intellectual Property: Reassessments of the Challenge and United States Policy," Update to the IP Commission Report, *National Bureau of Asian Research*, February 27, 2017. (http://www.ipcommission.org/report/IP_Commission_Report_Update_2017.pdf); Office of the United States Trade Representative, "2018 Special 301 Report," April 3, 2018. (https://ustr.gov/sites/default/files/files/Press/Reports/2018%20Special%20301.pdf); U.S.-China Economic and Security Review Commission, "2017 Annual Report," November 15, 2017. (https://www.uscc.gov/Annual_Reports/2017-annual-report); Michael Brown and Pavneet Singh, "China's Technology Transfer Strategy: How Chinese Investments in Emerging Technology Enable a Strategic Competitor to Access the Crown Jewels of U.S. Innovation," *Defense Innovation Unit Experimental*, January 2018. (https://admin.govexec.com/media/diux_chinatechnologytransferstudy_jan_2018_(1).pdf); Adam Segal and Alex Grigsby, "Cyber Operations Tracker," *Council on Foreign Relations*, accessed July 25, 2018. (https://www.cfr.org/interactive/cyber-operations)

4. This paper uses the term cyber-enabled economic espionage to encompass the subset of cyber espionage, as defined by Samantha Ravich and Annie Fixler, which affects the economic assets of a nation. As they explain, in order to determine if a cyber infiltration or attack is part of a cyber-enabled economic warfare campaign, it is necessary to understand the intentions of the attacker. This paper analyzes publicly available information to assess the intentions of the Chinese government. Samantha F. Ravich and Annie Fixler, "Framework and Terminology for Understanding Cyber-Enabled Economic Warfare," *Foundation for Defense of Democracies*, February 22, 2017. (http://www.defenddemocracy.org/content/uploads/documents/MEMO_CyberDefinitions_07.pdf)

5. For example, see: U.S. Department of Defense, "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2017," May 15, 2017. (https://www.defense.gov/Portals/1/Documents/pubs/2017_China_Military_Power_Report.PDF); Office of the United States Trade Representative, "2018 Special 301 Report," April 3, 2018. (https://ustr.gov/sites/default/files/files/Press/Reports/2018%20Special%20301.pdf); U.S.-China Economic and Security Review Commission, "2017 Annual Report," November 15, 2017. (https://www.uscc.gov/Annual_Reports/2017-annual-report)

6. Dennis C. Blair and Jon M. Huntsman, Jr., "The Report of the Commission on the Theft of American Intellectual Property," *National Bureau of Asian Research*, May 2013, page 3. (http://ipcommission.org/report/IP_Commission_Report_052213.pdf)

7. "2013 Data Breach Investigations Report," *Verizon*, 2013, page 21. (http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf)

property theft could cost over $300 billion annually to the U.S. economy.[8] The U.S.-China Economic and Security Review Commission has concluded that Chinese espionage "comprises the single greatest threat to U.S. technology."[9] Chinese espionage has not only damaged U.S. companies, but has also helped China save on research and development expenses while catching up in several critical industries. The cumulative effect of China's cyber-enabled economic espionage has been to "erode the United States' long term position as a world leader in [science and technology] innovation and competitiveness."[10] Perhaps most worryingly, China is reversing many of the U.S. military's technical and industrial advantages and creating potential vulnerabilities should a conflict arise.

At the same time, China has demonstrated a willingness to use cyber attacks as a tool of economic coercion to pressure governments and private companies to change their policies. In 2017, for example, after Washington and Seoul announced the deployment of the U.S. THAAD missile defense system to South Korea, the private Korean company on whose land the system was to be positioned suffered significant cyber attacks from China.[11]

Since 2015, the overall number of detected network breaches from China appears to have declined, but experts assess that Chinese cyber activity is "more focused, calculated and still successful in compromising corporate networks."[12] Although the response from the United States and its allies and partners has heretofore been inadequate, the post-2015 change in Chinese cyber activities indicates that concerted pressure can alter Beijing's behavior. A sustained campaign to demonstrate to Beijing that its malicious cyber activities will impair U.S.-China relations is likely the only way to convince the Chinese Communist Party to alter its behavior.[13]

"Chinese espionage has not only damaged U.S. companies, but has also helped China save on research and development expenses while catching up in several critical industries."

To develop effective policies to protect American innovation and the industrial base as well as change Chinese behavior, U.S. policymakers must better understand Chinese decision-making regarding cyber-enabled economic activities. This report reviews Beijing's use of cyber tools to accomplish its strategic objectives, analyzes the scope of Chinese cyber intrusions, and provides an open-source account of cyber-enabled economic intrusions to evaluate the damage these activities have caused in both economic and geostrategic terms. Only by understanding the scope of the campaign can the United States and its allies and partners develop effective strategies to deter and defend against Chinese cyber intrusions.

8. Dennis C. Blair and Jon M. Huntsman, Jr., "The Report of the Commission on the Theft of American Intellectual Property," *National Bureau of Asian Research*, May 2013, page 3. (http://ipcommission.org/report/IP_Commission_Report_052213.pdf); Council of Economic Advisors, "The Cost of Malicious Cyber Activity to the U.S. Economy," *The White House*, February 2018, page 4. (https://www.whitehouse.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf)

9. U.S.-China Economic and Security Review Commission, "2007 Report to Congress: Executive Summary," 2007, page 6. (https://www.uscc.gov/sites/default/files/annual_reports/2007-Report-to-Congress-Executive%20Summary.pdf)

10. Bryan Krekel, "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation," *U.S.-China Economic and Security Review Commission*, October 9, 2009, page 52. (https://nsarchive2.gwu.edu//NSAEBB/NSAEBB424/docs/Cyber-030.pdf)

11. Simon Atkinson, "Is China retaliating against Lotte missile deal?" *BBC News* (UK), March 6, 2017. (http://www.bbc.com/news/business-39176388)

12. "Redline Drawn: Cyber Recalculates its Use of Cyber Espionage," *FireEye*, June 2016, page 15. (https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf)

13. For example, see: Carlos Tejada, "Beg, Borrow or Steal: How Trump Says China Takes Technology," *The New York Times*, March 23, 2018. (https://www.nytimes.com/2018/03/22/business/china-trump-trade-intellectual-property.html)

China's Strategic Approach

[T]he Party has united and led all the Chinese people in a tireless struggle, propelling China into a leading position in terms of economic and technological strength, defense capabilities, and composite national strength. China's international standing has risen as never before. Our Party, our country, our people, our forces, and our nation have changed in ways without precedent. The Chinese nation, with an entirely new posture, now stands tall and firm in the East.

- Xi Jinping, 19th Party Congress (2017)[14]

China's cyber capabilities are the tools to achieve the strategic objectives of the Chinese Communist Party (CCP). The U.S. Department of Defense summarizes the CCP's primary goals as: 1) perpetuating CCP rule; 2) maintaining domestic stability; 3) sustaining economic growth and development; 4) defending national sovereignty and territorial integrity; 5) securing China's status as a great power and, ultimately, reacquiring regional preeminence; and 6) safeguarding China's interests abroad.[15] In recent years, the CCP has used cyber capabilities in the pursuit of each of these objectives.

The Role of Cyber in China's Search for Economic Security

The drive for indigenous innovation has motivated Beijing since the onset of market-oriented reforms in the late 1970s. In 1978, Deng Xiaoping's "four modernizations" policy aimed to speed development by prioritizing advances in agriculture, industry, science and technology, and defense. A key element of this effort began in March 1986 when Project 863 sought to narrow the gaps in computers, telecommunications, biotechnology, nanotechnology, and other areas by investing $200 billion in high-technology sectors.[16]

Despite its astounding growth and notable success in advanced manufacturing, China's economy remains down the value chain in many sectors. At the beginning of the current decade, the CCP expressed concern that "despite the size of our economy, our country is not an economic power, primarily because of our weak innovative capacity."[17] To rectify this problem and begin the "great renaissance of the Chinese nation," China issued the National Medium- and Long-Term Plan for the Development of Science and Technology (MLP) in 2010. The MLP prioritized innovation and technology in energy, water and mineral resources, environment, agriculture, manufacturing, transportation, information and services, population and health, urbanization, public security, and national defense. It called for Chinese nationals to author patents and publish leading academic papers to place China in the top five innovators in the world.[18]

In practice, writes Richard McGregor, the MLP has served as a "blueprint for technology theft on a scale the world has never seen before."[19] As Dean Cheng notes, "Chinese authorities have welcomed foreign direct investment in the PRC—but foreign companies are

14. Xi Jinping, "Report at 19th CPC National Congress," *China Daily*, October 18, 2017. (http://www.chinadaily.com.cn/china/19thcpcnationalcongress/2017-11/04/content_34115212.htm)
15. U.S. Department of Defense, "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2017," May 15, 2017, page 37. (https://www.defense.gov/Portals/1/Documents/pubs/2017_China_Military_Power_Report.PDF)
16. Evan A. Feigenbaum, *China's Techno-Warriors: National Security and Strategic Competition from the Nuclear to the Information Age* (Stanford, Calif: Stanford University Press, 2003); Office of the Director of National Intelligence, Office of the National Counterintelligence Executive, "Foreign Spies Stealing US Economic Secrets in Cyberspace," October 2011, pages 7-8. (https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/20111103_report_fecie.pdf)
17. "The National Medium- and Long-Term Plan for the Development of Science and Technology (2006-2020)" cited in James McGregor, "China's Drive for 'Indigenous Innovation': A Web of Industrial Policies," *U.S. Chamber of Commerce*, July 28, 2010, page 4. (https://www.uschamber.com/sites/default/files/documents/files/100728chinareport_0_0.pdf)
18. James McGregor, "China's Drive for 'Indigenous Innovation': A Web of Industrial Policies," *U.S. Chamber of Commerce*, July 28, 2010, page 15. (https://www.uschamber.com/sites/default/files/documents/files/100728chinareport_0_0.pdf)
19. Ibid, page 6.

generally required to form joint ventures with Chinese partners, who in turn will have access to key processes and intellectual property. The ability even to form a joint venture is often predicated upon the willingness to transfer technology, processes, or patents to the PRC."[20]

In 2011, leaders in Beijing started discussing a program called "Made in China 2025," which they adopted in 2013. Made in China 2025 seeks to transform China into a global leader in manufacturing through the use of industrial policy. Indigenous innovation, local production, controllable standards, and domestic brands are key to this strategy. The Made in China 2025 technical area road map for next generation information technology sets forth major goals for integrated circuits, information and telecommunication equipment, operating systems and industrial software, and core information equipment for smart manufacturing, among other areas. The strategy also sets ambitious targets, including that "40 percent of mobile phone chips on the Chinese market are supposed to be produced in China by 2025, as well as 70 percent of industrial robots and 80 percent of renewable energy equipment."[21]

In pursuit of economic security, Beijing employs the full array of cyber capabilities, which have helped it to build national champions in key industries, conduct industrial espionage, amass dual-use military technology, gain leverage in economic deals, restrict trade, and pressure foreign governments.[22] According to the U.S. intelligence community, "China's cyberspace operations are part of a complex, multipronged technology development strategy that uses licit and illicit methods to achieve its goals."[23] Similarly, a study conducted on behalf of the Pentagon by Michael Brown and Pavneet Singh explains that China acquires technology through illicit means, like industrial espionage, human intelligence, and cyber theft, as well as through legal ones, such as strategic investments, recruiting talent, using open-source information cataloguing foreign innovation, and acquiring knowledge through education in the United States and business deals with U.S. firms.[24] In 2017, the Pentagon stated that Beijing had conducted "an intensive campaign to obtain foreign technology through imports, foreign direct investment, industrial and cyberespionage, and establishment of foreign R&D centers."[25]

In addition, then-Secretary of Commerce Penny Pritzker noted in 2016, "We are seeing new attempts by China to acquire companies and technology based on their government's interests – not commercial objectives."[26] The impact in specific sectors could be substantial. For example, from 2013 through 2016, Chinese companies attempted a number of major acquisitions in the semiconductor industry, which

20. Dean Cheng, "China's S&T and Innovation Efforts," *Testimony before the House Armed Services Emerging Threats and Capabilities Subcommittee*, January 9, 2018, pages 4-5. (http://docs.house.gov/meetings/AS/AS26/20180109/106756/HHRG-115-AS26-Wstate-ChengD-20180109.pdf)

21. Jost Wübbeke, Mirjam Meissner, Max J. Zenglein, Jaqueline Ives, and Björn Conrad, "Made in China 2025: The making of a high-tech superpower and consequences for industrial countries," *Mercator Institute for China Studies*, December 2016, page 7. (https://www.merics.org/sites/default/files/2017-09/MPOC_No.2_MadeinChina2025.pdf)

22. Such actions may also create weaknesses in the U.S. industrial base that can be leveraged in a crisis or conflict.

23. Office of the Director of National Intelligence, National Counterintelligence and Security Center, "Foreign Economic Espionage in Cyberspace," July 26, 2018, page 5. (https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf)

24. Michael Brown and Pavneet Singh, "China's Technology Transfer Strategy: How Chinese Investments in Emerging Technology Enable a Strategic Competitor to Access the Crown Jewels of U.S. Innovation," *Defense Innovation Unit Experimental*, January 2018, pages 3, 17-21. (https://admin.govexec.com/media/diux_chinatechnologytransferstudy_jan_2018_(1).pdf)

25. U.S. Department of Defense, "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China," May 15, 2017, page 72. (https://www.defense.gov/Portals/1/Documents/pubs/2017_China_Military_Power_Report.PDF)

26. Penny Pritzker, "Major Policy Address on Semiconductors," *Remarks at the Center for Strategic and International Studies*, November 2, 2016. (https://www.commerce.gov/news/secretary-speeches/2016/11/us-secretary-commerce-penny-pritzker-delivers-major-policy-address)

together were valued over $37 billion.[27] As Pritzker observed, "In 2014, the Chinese Government announced that it would spend $150 billion to expand the share of Chinese-made integrated circuits in its market from 9 percent to 70 percent by 2025. To put that figure into perspective, $150 billion is roughly half of all worldwide semiconductor sales last year."[28] Given the critical role the semiconductors play in advanced military systems, Chinese dominance in that industry could fundamentally alter the military balance.

"China-based investors seem particularly interested in artificial intelligence, robotics, augmented reality/virtual reality, and financial technology. Products based on these technologies have both commercial and military applications."

This kind of Chinese investment activity in the United States could undermine long-term U.S. economic and military competitiveness. Estimates suggest that China participates in 10-16 percent of all venture capital deals, including 271 early-state technology investment deals worth $11.5 billion in 2015 alone.[29] In a number of cases, American companies – including many specialized in technology that has military applications – have turned to China for funding.[30] For example, artificial intelligence company Neurala struggled to get funding from the U.S. military and instead accepted funding from a Chinese group associated with a state-owned company. In another case, Quanergy, which develops sensors for military applications, accepted venture funding from the Chinese fund GP Capital.[31] In a third case, China's State Council reportedly financed an initial investment in Canyon Bridge Capital Partners in its attempted $1.3 billion takeover of Lattice Semiconductor, which was later blocked by the Trump administration on national security grounds.[32]

Given the Chinese government's embrace of military-civil fusion and the fact that many of the technologies in which China is investing are central to the Pentagon's efforts to maintain technological superiority, these types of investments suggest that U.S. technology could be used for Chinese military purposes. Key defense-related targets reportedly include "sensitive or military-grade equipment" such as accelerometers, radiation hardened programmable semiconductors and computer circuits, military sensors, restricted microwave amplifiers, high-grade carbon fiber, proprietary and export-restricted technical data, and thermal imaging systems. China-based investors seem particularly interested in artificial intelligence, robotics, augmented reality/virtual reality, and financial technology. Products

27. Thilo Hanemann and Daniel H. Rosen, "Chinese Investment in the United States: Recent Trends and the Policy Agenda," *U.S.-China Economic and Security Review Commission*, December 2016, pages 79-80. (https://www.uscc.gov/sites/default/files/Research/Chinese_Investment_in_the_United_States_Rhodium.pdf)

28. Penny Pritzker, "Major Policy Address on Semiconductors," *Remarks at the Center for Strategic and International Studies*, November 2, 2016. (https://www.commerce.gov/news/secretary-speeches/2016/11/us-secretary-commerce-penny-pritzker-delivers-major-policy-address)

29. Michael Brown and Pavneet Singh, "China's Technology Transfer Strategy: How Chinese Investments in Emerging Technology Enable a Strategic Competitor to Access the Crown Jewels of U.S. Innovation," *Defense Innovation Unit Experimental*, January 2018, pages 7-8. (https://admin.govexec.com/media/diux_chinatechnologytransferstudy_jan_2018_(1).pdf); See also: "China Investment Monitor," *Rhodium Group*, accessed August 17, 2018. (https://rhg.com/research/china-investment-monitor/)

30. On the other hand, China maintains strict processes for inbound investment. For example, see: U.S. Chamber of Commerce, "China's Approval Process for Inbound Foreign Direct Investment: Impact on Market Access, National Treatment and Transparency," 2012. (https://www.uschamber.com/sites/default/files/legacy/reports/020021_China_InvestmentPaper_hires.pdf)

31. Paul Mozur and Jane Perlez, "China Bets on Sensitive U.S. Start-Ups, Worrying the Pentagon," *The New York Times*, March 22, 2017. (https://www.nytimes.com/2017/03/22/technology/china-defense-start-ups.html)

32. The deal was later blocked by the U.S. government. Liana B. Baker, Koh Gui Qing, and Julie Zhu, "Exclusive: Chinese government money backs buyout firm's deal for U.S. chip maker," *Reuters*, November 28, 2016. (https://www.reuters.com/article/us-lattice-m-a-canyonbridge/exclusive-chinese-government-money-backs-buyout-firms-deal-for-u-s-chip-maker-idUSKBN13N1D5)

based on these technologies have both commercial and military applications.[33]

It should be noted that Chinese experts have tended not to distinguish espionage directed against governments from espionage directed against commercial targets.[34] In particular, the United States and China take opposing views on the legitimacy of state-directed economic or industrial espionage.[35] Chinese experts also tend to view corporate cyber-enabled espionage more permissively, regardless of whether it is state-directed.

Chinese Perceptions of the Cyber Domain as a Theater of Military Competition

The Cyberspace Administration of China states that the PRC seeks to become a "cyber superpower."[36] From Beijing's perspective, the aggressive exploitation of the cyber domain by the United States and Russia, among other actors, necessitates more advanced capabilities. More broadly, the U.S. military's superior ability to use information to gain battlefield advantage has convinced many in Beijing of the importance of a renewed Chinese investment in networked forces.[37] To compensate for the U.S. lead in most military technology, Beijing pursues asymmetric approaches, such as "informatized warfare," whose purpose is to level the playing field. Cyber capabilities are integral to this effort.

Many in China see American concerns about Beijing's cyber conduct as an attempt to distract attention from America's own provocations and thirst for cyber dominance. Michael Swaine finds that "non-authoritative Chinese sources are particularly voluble and energetic in their criticism of the United States for four alleged sins related to its never-ending search for hegemony: 1) the militarization of cyberspace; 2) the pursuit of a double standard in claiming cyberfreedom for itself while attacking or limiting such freedom for others; 3) engaging in completely groundless, destructive, and self-serving accusations against China; and 4) unfairly dominating the current global cybersystem."[38] Chinese scholars frequently cite data from the Chinese Ministry of Defense, which claims that 63 percent of attempts to hack People's Liberation Army (PLA) military websites originate in the United States.[39]

Meanwhile, Chinese leaders often argue that they are only building capabilities for deterrence and defense, not for offense. For example, China's 2015 Defense White Paper states that China "will not attack [in cyber space] unless we are attacked; but we will surely

33. Michael Brown and Pavneet Singh, "China's Technology Transfer Strategy: How Chinese Investments in Emerging Technology Enable a Strategic Competitor to Access the Crown Jewels of U.S. Innovation," *Defense Innovation Unit Experimental*, January 2018, pages 1, 2, and 5. (https://admin.govexec.com/media/diux_chinatechnologytransferstudy_jan_2018_(1).pdf)

34. Kimberly Hsu and Craig Murray, "China and International Law in Cyberspace," *U.S.-China Economic and Security Review Commission Staff Report*, May 6, 2014, page 6. (https://www.uscc.gov/sites/default/files/Research/China%20International%20Law%20in%20Cyberspace.pdf)

35. Scott Warren Harold, Martin C. Libicki, and Astrid Stuth Cevallos, "The 'Cyber Problem' in U.S.-China Relations," in *Getting to Yes with China in Cyberspace* (Santa Monica, Calif.: RAND Corporation, 2016), page 6. (http://www.jstor.org/stable/10.7249/j.ctt1cx3vfr.6); Julian Ku, "How China's Views on the Law of *Jus ad Bellum* Will Shape Its Legal Approach to Cyberwarfare," *Hoover Institution*, August 17, 2017. (https://www.hoover.org/sites/default/files/research/docs/ku_webreadypdf.pdf)

36. Elsa Kania, Samm Sacks, Paul Triolo, and Graham Webster, "China's Strategic Thinking on Building Power in Cyberspace," *New America*, September 25, 2017. (http://www.newamerica.org/cybersecurity-initiative/blog/chinas-strategic-thinking-building-power-cyberspace/)

37. Dean Cheng, "China's S&T and Innovation Efforts," *Testimony before the House Armed Services Emerging Threats and Capabilities Subcommittee*, January 9, 2018, pages 4-5. (http://docs.house.gov/meetings/AS/AS26/20180109/106756/HHRG-115-AS26-Wstate-ChengD-20180109.pdf)

38. Michael Swaine, "Chinese Views on Cybersecurity in Foreign Relations," *China Leadership Monitor*, July 30, 2013, page 14. (http://carnegieendowment.org/email/South_Asia/img/CLM42MSnew.pdf)

39. Bill French, "China and the Cyber Great Game," *The National Interest*, March 20, 2013. (http://nationalinterest.org/commentary/china-the-cyber-great-game-8241)

counterattack if needed."[40] Since it is difficult to differentiate defensive capabilities from offensive ones, Beijing's public commitment to a defensive strategy may not limit its options. As Bryan Krekel notes, "the only distinction between computer network exploitation and attack is the intent of the operator at the keyboard. The skill sets needed to penetrate a network for intelligence gathering purposes in peacetime are the same skills necessary to penetrate that network for offensive action during wartime."[41] In recent years, PLA writings also analyze the advantage of consolidating offensive and defensive cyber capabilities, and the U.S. Defense Department assesses that this may be one of China's goals in creating its Strategic Support Force.[42]

Chinese military strategists argue that a disruptive cyber attack on the U.S. military's communications, transportation, and logistics systems and the related civilian systems would degrade U.S. capabilities, and believe that the U.S. military's reliance on civilian infrastructure is a key weakness they can exploit.[43] A 2015 PLA white paper identified cyber space as one of four "critical security domains," and in wartime, cyber capabilities can "ensure victory on the battlefield," stated a PLA scholar.[44] Thus, Chinese cyber operations against the U.S. homeland might be one of the PLA's most attractive military options in a major conflict. The Defense Department warns of "Chinese military planners' work to build a picture of U.S. defense networks, logistics, and related military capabilities that could be exploited during a crisis." Furthermore, the Pentagon has suggested that "the PLA may seek to use its cyberwarfare capabilities to collect data for intelligence and cyberattack purposes; to constrain an adversary's actions by targeting network-based logistics, communications, and commercial activities; or to serve as a force multiplier when coupled with kinetic attacks during times of crisis or conflict."[45]

Cyber operations comprise one element of a broader Chinese effort to execute "informatized warfare," which Chinese military writings describe as "an asymmetric way to weaken an adversary's ability to acquire, transmit, process, and use information during war and to force an adversary to capitulate before the onset of conflict."[46] According to President Xi, China must "improve combat capabilities for joint operations based on the network information system and the ability to fight under multi-dimensional conditions."[47] Thus, cyber is a critical part of China's emerging military strategy.

Specifically, Chinese military documents assert that establishing information dominance and control of an enemy's information flow is a prerequisite for air and naval superiority.[48] In that regard, the U.S. Department of Defense has warned, "PLA researchers advocate seizing 'cyberspace superiority' by using offensive cyber

40. "Full Text: China's Military Strategy," *Xinhua News Agency* (China), May 26, 2015. (http://www.xinhuanet.com/english/china/2015-05/26/c_134271001_3.htm)
41. Bryan Krekel, "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation," *U.S.-China Economic and Security Review Commission*, October 9, 2009, pages 8-9. (https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-030.pdf)
42. U.S. Department of Defense, "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China," May 15, 2017, page 35. (https://www.defense.gov/Portals/1/Documents/pubs/2017_China_Military_Power_Report.PDF)
43. James Mulvenon, "PLA Computer Network Operations: Scenarios, Doctrine, Organizations, and Capability," *Beyond the Strait: PLA Missions Other Than Taiwan*, Eds. Roy Kamphausen, David Lai, and Andrew Scobell (Carlisle, PA: Army War College Strategic Studies Institute, 2009), pages 269-270. (http://indianstrategicknowledgeonline.com/web/Ch_8-1.pdf)
44. U.S. Department of Defense, "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China," May 15, 2017, page 35. (https://www.defense.gov/Portals/1/Documents/pubs/2017_China_Military_Power_Report.PDF)
45. Ibid, pages 59-64.
46. Ibid, page 58.
47. Xi Jinping, "Report at 19th CPC National Congress," *China Daily*, October 18, 2017. (http://www.chinadaily.com.cn/china/19thcpcnationalcongress/2017-11/04/content_34115212.htm)
48. *The Science of Campaigns*, Eds. Wang Houqing and Zhang Xingye (Washington, DC: National Defense University Press, 2000); *The Science of Military Strategy*, Eds. Peng Guangqiang and Yao Youzhi, (Military Science Publishing House, 2005)

operations to deter or degrade an adversary's ability to conduct military operations against China."[49] Although cyber attacks on critical infrastructure would likely cause human casualties, some Chinese military strategy documents describe cyber attacks as "bloodless" and suggest that they may be "first choice weapons for a limited strike against adversary targets to deter further escalation of a crisis."[50]

Chinese military leaders, including the former head of the department that handles electronic warfare, have noted that "[i]nformation operations in high-tech warfare are, to a very great extent, a struggle which revolves around the destruction and the protection of C4ISR [command, control, communications, computers, intelligence, surveillance, and reconnaissance] systems."[51] Command-and-control targets are particularly attractive, with an article in the PLA's Science of Information Operations observing that when "a virus enters the enemy's command and control system, it will have tremendous destructive impact."[52] As researchers at the RAND Corporation conclude, "Perhaps no U.S. military vulnerability is as important, in Chinese eyes, as its heavy reliance on its information network. … Successfully attacking that system will affect U.S. combat capabilities much more profoundly than would directly targeting combat platforms. Chinese strategists also believe that the U.S. military information network is not just vulnerable but also fragile. Thus, the foundation of the U.S. military's success can also be its undoing."[53]

Key Chinese Actors

Chinese actors are the world's most active and persistent perpetrators of economic espionage.

- U.S. Office of the National Counterintelligence Executive (2011)[54]

The resources China devotes to cyber activities are massive. The Chinese campaigns are of such a large scale that most experts believe they require "some type of state-sponsorship."[55] The FBI estimates that China has more than 30,000 military cyber spies, plus an additional 150,000 private sector cyber experts "whose mission is to steal American military and technological secrets," according to former head of U.S. counterintelligence Michelle Van Cleave.[56]

Although Chinese officials frequently dispute foreign accusations that the PRC is involved in malicious cyber activities, there is robust evidence that specific actors

49. U.S. Department of Defense, "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China," May 15, 2017, page 51. (https://www.defense.gov/Portals/1/Documents/pubs/2017_China_Military_Power_Report.PDF)
50. Bryan Krekel, "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation," *U.S.-China Economic and Security Review Commission*, October 9, 2009, page 19. (https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-030.pdf); See also: Adam P. Liff, "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War," *Journal of Strategic Studies*, June 1, 2012, pages 401-428. (https://www.tandfonline.com/doi/abs/10.1080/01402390.2012.663252)
51. Dai Qingmin, "On Integrating Network Warfare and Electronic Warfare," *China Military Science*, February 1, 2002, pages 112-117.
52. Quoted in: Kevin Pollpeter, "Chinese Writings on Cyberwarfare and Coercion," *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, Eds. Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron (Oxford University Press: New York, 2015).
53. Roger Cliff, Evan Medeiros, and Keith Crane, "Keeping the Pacific: An American Response to China's Growing Military Might," *RAND Corporation*, Spring 2007. (https://www.rand.org/pubs/periodicals/rand-review/issues/spring2007/pacific.html)
54. Office of the National Counterintelligence Executive "Foreign Spies Stealing US Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage," October 2011, page i. (https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/20111103_report_fecie.pdf)
55. Bryan Krekel, "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation," *U.S.-China Economic and Security Review Commission*, October 9, 2009, page 8. (https://nsarchive2.gwu.edu//NSAEBB/NSAEBB424/docs/Cyber-030.pdf)
56. Michelle Van Cleave, "Chinese Intelligence Operations and Implications for U.S. National Security," *Testimony before the U.S.-China Economic and Security Review Commission*, June 9, 2016, page 5. (https://www.uscc.gov/sites/default/files/Michelle%20Van%20Cleave_Written%20Testimony060916.pdf)

within China – and within the Chinese government – have often been responsible. China's cyber groups "operate partially at the behest of the PLA through a dual civil-military command structure,"[57] and the state has consolidated control over some private cyber actors.[58] There are allegations of direct ties between the Politiburo Standing Committee and China's cyber attacks, which were revealed via the publication of U.S. government cables eight years ago. According to the cables, Li Changchun, then a member of the Politburo Standing Committee, may have overseen hacking against Google through the State Council Information Office, along with fellow Politburo Standing Committee member Zhou Yongkang.[59] To carry out such intrusions, Dean Cheng argues, "there are three broad categories of Chinese computer network warfare forces… 1) Specialized military units, specifically tasked for implementing network offensive and defensive operations; 2) Specialist units organized with military permission, drawn from local capabilities (e.g., from within a military region or war zone), including the Ministry of State Security and the Ministry of Public Security, and other relevant government departments; and 3) Civilian strength, comprised of voluntary civilian participants who can conduct network operations after being mobilized and organized."[60]

Before the establishment of China's Strategic Support Force (SSF) in December 2015, China operated cyber exploitation and attack units that reported to the Central Military Commission, the State Council (through the Ministry of State Security), and other groups.[61] The PLA's "Integrated Network Electronic Warfare" strategy combined offensive computer network attacks and electronic warfare as part of the PLA General Staff Department's 4th Department, also known as the Electronic Countermeasures Department (4PLA). Computer network defense and intelligence gathering responsibilities likely belonged to the 3rd Department (3PLA), Signals Intelligence Department, as well as specialized information warfare militia units.[62] 3PLA was also responsible for technical reconnaissance before the establishment of the SSF.[63]

The SSF is now responsible for the PLA's cyber mission (along with electronic warfare and space warfare).[64] While it appears that the missions of both 4PLA and 3PLA have shifted to the SSF Network Systems Department, along with many of the sub-units and much of the leadership, the precise organizational structure is not available in unclassified reporting. The two units most often associated with China's

57. Robert Sheldon and Joe McReynolds, "Civil-Military Integration and Cybersecurity: A Study of Chinese Information Warfare Militias," *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, Eds. Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron (Oxford University Press: New York, 2015), page 193.

58. For a detailed study on China's use of cyber proxies and the changes over the past three decades, see: Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge University Press: New York, 2018), Chapter 7.

59. James Glanz and John Markoff, "WikiLeaks Archive - China's Battle With Google," *The New York Times*, December 4, 2010. (http://www.nytimes.com/2010/12/05/world/asia/05wikileaks-china.html?pagewanted=all)

60. Dean Cheng, "China's S&T and Innovation Efforts," *Testimony before the House Armed Services Emerging Threats and Capabilities Subcommittee*, January 9, 2018, page 7. (http://docs.house.gov/meetings/AS/AS26/20180109/106756/HHRG-115-AS26-Wstate-ChengD-20180109.pdf)

61. Robert Windrem, "China Read Emails of Top U.S. Officials," *NBC News*, August 10, 2015. (https://www.nbcnews.com/news/us-news/china-read-emails-top-us-officials-n406046)

62. Bryan Krekel, "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation," *U.S.-China Economic and Security Review Commission*, October 9, 2009, pages 6-7. (https://nsarchive2.gwu.edu//NSAEBB/NSAEBB424/docs/Cyber-030.pdf)

63. Mark A. Stokes, "The PLA General Staff Department Third Department Second Bureau: An Organizational Overview of Unit 61398," *Project 2049 Institute*, July 27, 2015. (https://www.documentcloud.org/documents/2849768-Document-09.html)

64. For more information on the Strategic Support Force, see: John Costello, "The Strategic Support Force: Update and Overview," *The Jamestown Foundation*, December 21, 2016. (https://jamestown.org/program/strategic-support-force-update-overview/); Elsa Kania, "PLA Strategic Support Force: The 'Information Umbrella' for China's Military," *The Diplomat*, April 1, 2017. (https://thediplomat.com/2017/04/pla-strategic-support-force-the-information-umbrella-for-chinas-military/)

operations in cyber space have been Units 61398 and 61486,[65] both of which resided within the 3PLA and were based in the Shanghai area.[66] Since the creation of the SSF, it is unclear where in the hierarchy these two units now reside.

"Previously, cyber security firm Mandiant had published an analysis of attacks conducted by an entity it labeled Advanced Persistent Threat 1 (APT1), also known as Unit 61398. Mandiant researchers concluded, 'APT1 is likely government-sponsored and one of the most persistent of China's cyber threat actors'."

Thanks to a federal indictment of five of its officers, a great deal more is known about Unit 61398. In May 2014, the U.S. Department of Justice indicted them for "computer hacking, economic espionage and other offenses" against U.S. nuclear power, metals, and solar industries.[67] According to the indictment, individuals associated with Unit 61398 "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)."[68] Previously, cyber security firm Mandiant had published an analysis of attacks conducted by an entity it labeled Advanced Persistent Threat 1 (APT1), also known as Unit 61398. Mandiant researchers concluded, "APT1 is likely government-sponsored and one of the most persistent of China's cyber threat actors. We believe that APT1 is able to wage such a long-running and extensive cyber espionage campaign in large part because it receives direct government support."[69]

Mandiant observed that APT1 and Unit 61398 shared missions, capabilities, resources, and locations. Unit 61398 operated from a 12-story, 130,000-square-foot facility in Pudong New Area, which also happened to be one of the main operating centers for APT1. Additionally, 98 percent of APT1's internet protocol addresses resolved back to China. The overwhelming majority of these addresses are registered to four networks in Shanghai. In 97 percent of remote desktop sessions, the APT1 intruders used Chinese language keyboards. As a result, Mandiant researchers concluded, "We believe the totality of the evidence we provide in this document bolsters the claim that APT1 is Unit 61398." The industries APT1 targeted "match industries that China has identified as strategic to their growth." APT1 has been observed stealing "intellectual property, including technology blueprints, proprietary manufacturing processes, test results, business plans, pricing documents, partnership agreements, and emails and contact lists from victim organizations' leadership." From 2006 to 2013, researchers at Mandiant observed

65. Mikk Raud, "China and Cyber: Attitudes, Strategies, Organisation," *NATO Cooperative Cyber Defence Centre of Excellence*, 2016. (https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_CHINA_092016.pdf)

66. "Hat-tribution to PLA Unit 61486," *CrowdStrike*, June 9, 2014. (https://www.crowdstrike.com/blog/hat-tribution-pla-unit-61486/); "APT1: Exposing One of China's Cyber Espionage Units," *Mandiant*, February 19, 2013. (https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf)

67. According to the indictment, from 2006 through 2014, Wang Dong, Sun Kailiang, Wen Xinyu, Huang Zhenyu, and Gu Chunhui conducted intrusions against Westinghouse, SolarWorld, U.S. Steel, Allegheny Technologies, Alcoa, and the United Service Workers union. The indictment included 31 counts, including one computer fraud count, eight unauthorized computer access counts, 14 transmissions intended to cause harm counts, six aggravated identity theft counts, one economic espionage count, and one trade secret theft count. U.S. Department of Justice, Press Release, "U.S. Charges Five Chinese Military Hackers for Cyber Espionage," May 19, 2014. (https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor)

68. U.S. Department of Justice, Press Release, "U.S. Charges Five Chinese Military Hackers for Cyber Espionage," May 19, 2014. (https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor)

69. "APT1: Exposing One of China's Cyber Espionage Units," *Mandiant*, February 19, 2013, page 2. (https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf)

compromises of 141 companies in 20 industries by APT1 alone.[70]

"Differentiating military from civilian groups is often difficult; the line itself may be blurry, since Chinese writings highlight the importance of 'civil-military integration for cybersecurity and informatization.'"

Other malicious cyber actors in China also appear to have military or government connections. The aforementioned Unit 61486 has conducted multiple attacks against satellite, aerospace, and communications firms since 2007. Unit 61486 is also known as APT2 and is believed to support the Chinese space surveillance network.[71] APT10 is also believed to be a China-based cyber espionage group. A PwC and BAE Systems study of the group and its attacks on managed IT systems providers – a campaign dubbed "Operation Cloud Hopper" – found that the group has been operational since at least 2009.[72] While previously the group targeted the U.S. defense industrial base, as well as the technology and telecommunications sectors, in recent years it began targeting a broader range of industries by compromising IT service providers. Other groups linked to the PLA include APT3 (Gothic Panda), APT12 (Numbered Panda), APT15 (Vixen Panda), APT19 (Deep Panda), APT30 (believed to be PLA Unit 78020), Aurora, Shady RAT, and NightDragon.[73] Experts have identified dozens of other organizations that may also belong on the list.[74]

While some of these threat groups consist of military units, civilians – including those in the private sector – also play a critical role. FBI Director Christopher Wray has explained, "the Chinese government works hand in hand with Chinese companies, and others, to do everything they can, through all sorts of means, to try to steal our trade secrets, our economic assets."[75] As a result, differentiating military from civilian groups is often difficult; the line itself may be blurry, since Chinese writings highlight the importance of "civil-military integration for cybersecurity and informatization."[76]

China's Malicious Cyber Activities

China's cyber activities represent a grave threat to U.S. competitiveness and the U.S. economy.

- U.S. Trade Representative Investigation (2018)[77]

Qualitative analyses frequently invoke former National Security Agency Director Keith Alexander's comment that the cyber theft of economic information is

70. "APT1: Exposing One of China's Cyber Espionage Units," *Mandiant*, February 19, 2013. (https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf)
71. APT2 is also knowns as Putter Panda. "CrowdStrike Intelligence Report: Putter Panda," *CrowdStrike*, June 2014. (https://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf)
72. "Operation Cloud Hopper," *PwC UK and BAE Systems*, April 2017. (https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-report-final-v4.pdf)
73. James Scott, *China's Espionage Dynasty: Economic Death by a Thousand Cuts* (Institute for Critical Infrastructure Technology, 2016).
74. For example, see: "Cyber Campaigns Central," *Cyber Campaigns*, accessed July 25, 2018. (http://cybercampaigns.net)
75. "FBI Director Christopher Wray speaks with NBC News in extended interview," *NBC News*, March 22, 2018. (https://www.nbcnews.com/video/fbi-director-christopher-wray-speaks-with-nbc-news-in-extended-interview-1192723011704)
76. Elsa Kania, Samm Sacks, Paul Triolo, and Graham Webster, "China's Strategic Thinking on Building Power in Cyberspace," *New America*, September 25, 2017. (http://www.newamerica.org/cybersecurity-initiative/blog/chinas-strategic-thinking-building-power-cyberspace/)
77. Office of the United States Trade Representative, "Findings of the Investigation into China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation Under Section 301 of the Trade Act of 1974," March 22, 2018. (https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF)

"the greatest transfer of wealth in human history."[78] Former Director of National Intelligence Mike McConnell, former Secretary of Homeland Security Michael Chertoff, and former Deputy Secretary of Defense William Lynn put it succinctly: "The Chinese government has a national policy of economic espionage in cyberspace."[79] The extent of the hacking is extreme. In July 2018, FBI Director Christopher Wray revealed that the FBI is investigating economic espionage cases traced to China in every U.S. state.[80] In 2013, Verizon concluded that 96 percent of espionage-motivated cyber intrusions through its networks were conducted by China.[81]

Former FBI Director James Comey has stated, "There are two kinds of big companies in the United States; there are those who've been hacked by the Chinese and those who don't know they've been hacked by the Chinese."[82] One private firm reported 128 cyber intrusions per minute from China against U.S. targets.[83] In 2013 alone, the federal government alerted 3,000 companies that they had been hacked, most by Chinese groups.[84] Although much attention focuses on large companies, small companies suffer nearly four times the per capita cost.[85] Symantec estimates that 65 percent of all attacks target companies with less than 2,500 employees.[86] Indeed, an increasing number of intrusions are targeting smaller firms, as larger organizations improve their cyber defenses.

A central challenge in quantitative assessments of economic damage caused by cyber attacks is that most cyber incidents go unreported and many companies do not admit losses.[87] One study estimates that only 44 percent of victim companies report attacks.[88] Many others remain unaware of the attacks they are suffering. Classified U.S. assessments reportedly have significantly more detail on the number, type, and severity of China's malicious cyber intrusions – information critical to evaluating Beijing's revealed intentions and strategy. Yet, this information rarely becomes public due to the sensitivity of releasing information about U.S. efforts to monitor these activities, as well as the commercial risk of identifying damage to specific businesses.

78. Emil Protalinski, "NSA: Cybercrime Is 'the Greatest Transfer of Wealth in History,'" *ZDNet*, July 10, 2012. (http://www.zdnet.com/article/nsa-cybercrime-is-the-greatest-transfer-of-wealth-in-history/)
79. Mike McConnell, Michael Chertoff, and William Lynn, "China's Cyber Thievery Is National Policy—And Must Be Challenged," *The Wall Street Journal*, January 27, 2012. (https://www.wsj.com/articles/SB10001424052970203718504577178832338032176)
80. Tara Francis Chan, "FBI director calls China 'the broadest, most significant' threat to the US and says its espionage is active in all 50 states," *Business Insider*, July 19, 2018. (https://www.businessinsider.com/fbi-director-says-china-is-the-broadest-most-significant-threat-to-the-us-2018-7)
81. "2013 Data Breach Investigations Report," *Verizon*, 2013, page 21. (http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf)
82. "FBI Director on Threat of ISIS, Cybercrime," *CBS News*, October 5, 2014. (https://www.cbsnews.com/news/fbi-director-james-comey-on-threat-of-isis-cybercrime/)
83. Desmond Ball, "China's Cyber Warfare Capabilities," *Security Challenges*, Winter 2011, page 88. (https://indianstrategicknowledgeonline.com/web/china%20cyber.pdf)
84. "Net Losses: Estimating the Global Cost of Cybercrime," *Center for Strategic and International Studies and McAfee*, June 2014, page 4. (https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf)
85. "Second Annual Cost of Cyber Crime Study: Benchmark Study of U.S. Companies," *Ponemon Institute*, August 2011. (https://www.ponemon.org/local/upload/file/2011_2nd_Annual_Cost_of_Cyber_Crime_Study%20.pdf)
86. "Attackers Target both Large and Small Businesses," *Symantec*, accessed July 26, 2018. (https://www.symantec.com/content/dam/symantec/docs/infographics/istr-attackers-strike-large-business-en.pdf)
87. "Net Losses: Estimating the Global Cost of Cybercrime," *Center for Strategic and International Studies and McAfee*, June 2014, page 4. (https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf)
88. CERT Australia study cited in: "Net Losses: Estimating the Global Cost of Cybercrime," *Center for Strategic and International Studies and McAfee*, June 2014, page 6. (https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf)

American Victims of the Chinese Communist Party's Use of Cyber-Enabled Economic Warfare

Intellectual Property Theft

The U.S. Department of Defense notes, "China is using its cyber capabilities to support intelligence collection against the U.S. diplomatic, economic, and defense industrial base sectors. The information targeted can be used to benefit China's defense high-technology industries, support China's military modernization, or provide the CCP insights into U.S. leadership perspectives."[89]

Titan Rain, the first reported major Chinese intrusion, targeted Defense Department laboratories, NASA, and aerospace companies in 2003. Today, Chinese cyber attacks target nearly all technologies necessary for U.S. military superiority, according to former head of U.S. counterintelligence Michelle Van Cleave.[90] It is no surprise that the Made in China 2025 sectors match closely with the priorities of Chinese hackers. The areas of greatest Chinese interest are reported to be information and communications technology; military technology – including marine and aerospace; civilian and dual-use technologies – clean technologies, advanced materials, manufacturing techniques, healthcare, pharmaceuticals, and agricultural; and business – energy and natural resources, business deals, and macroeconomic information.[91]

A *Washington Post* summary of a classified 2013 U.S. National Intelligence Estimate on economic cyber espionage concluded, "China was by far the most active country in stealing intellectual property from U.S. companies."[92] In just two years between 2011 and 2013, U.S. companies reporting material damage from intellectual property infringement to their operations rose from 18 to 48 percent.[93] A 2015 FBI survey of dozens of victims of intellectual property theft found that 95 percent of companies accused China of being responsible for the hacks.[94]

Jon Lindsay argues that "worries about a wholesale erosion of U.S. defense competitiveness resulting from cyber espionage … are premature."[95] Yet the Mercator Institute for China Studies warns that "if Chinese enterprises prove capable of using [foreign] technology effectively, a hollowing out of the technology leadership of industrial countries in pillar industries is possible."[96]

In 2017, President Trump initiated a U.S. Trade Representative (USTR) investigation into Chinese trade practices and policies regarding technology

89. U.S. Department of Defense, "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2017," May 15, 2017, page 59. (https://www.defense.gov/Portals/1/Documents/pubs/2017_China_Military_Power_Report.PDF)
90. Michelle Van Cleave, "Chinese Intelligence Operations and Implications for U.S. National Security," *Testimony before the U.S.-China Economic and Security Review Commission*, June 9, 2016, page 5. (https://www.uscc.gov/sites/default/files/Michelle%20Van%20Cleave_Written%20Testimony060916.pdf)
91. Office of the Director of National Intelligence, Office of the National Counterintelligence Executive, "Foreign Spies Stealing US Economic Secrets in Cyberspace," October 2011. (https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/20111103_report_fecie.pdf)
92. Ellen Nakashima, "Confidential report lists U.S. weapons system designs compromised by Chinese cyberspies," *The Washington Post*, May 27, 2013. (https://www.washingtonpost.com/world/national-security/confidential-report-lists-us-weapons-system-designs-compromised-by-chinese-cyberspies/2013/05/27/a42c3e1c-c2dd-11e2-8c3b-0b5e9247e8ca_story.html)
93. "China Business Climate Survey Report," *American Chamber of Commerce in the People's Republic of China*, 2011; "China Business Climate Survey Report," *American Chamber of Commerce in the People's Republic of China*, 2013, (https://media.npr.org/documents/2013/may/AmChamSurvey.pdf)
94. Shane Harris, "FBI Probes 'Hundreds' of China Spy Cases," *The Daily Beast*, July 23, 2015. (https://www.thedailybeast.com/fbi-probes-hundreds-of-china-spy-cases)
95. Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron, *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain* (Oxford University Press: New York, 2015), page 26.
96. Jost Wübbeke, Mirjam Meissner, Max J. Zenglein, Jaqueline Ives, and Björn Conrad, "Made in China 2025: The making of a high-tech superpower and consequences for industrial countries," *Mercator Institute for China Studies*, December 2016, page 54. (https://espas.secure.europarl.europa.eu/orbis/sites/default/files/generated/document/en/MPOC_No.2_MadeinChina_2025.pdf)

transfer and intellectual property.[97] China had previously been on the USTR Priority Watch List due to its "widespread infringing activity, including trade secret theft, rampant online piracy and counterfeiting, and high levels of physical pirated and counterfeit exports to markets around the globe."[98] Among other conclusions, the report found that Chinese malicious cyber activities "represent a grave threat to U.S. competitiveness and the U.S. economy."[99]

"U.S. allies and partners also suffer considerable damage because of Chinese cyber attacks. … The effect in Germany has been particularly significant. … In just one month, a single German telecommunications firm reported over 30,000 Chinese cyber attacks. Estimates indicate that German firms lose $28-71 billion annually as a result."

U.S. allies and partners also suffer considerable damage because of Chinese cyber attacks. South Korea estimated in 2008 that foreign economic espionage cost its companies $82 billion. A 2007 survey in Japan found that 35 percent of manufacturing firms reported technology losses, with 60 percent involving China. In 2010, 86 percent of large Canadian corporations reported having been the victim of cyber espionage. Estimates in the United Kingdom indicate that industrial espionage and cyber attacks cost $34 billion per year.[100]

The effect in Germany has been particularly significant, given that Made in China 2025 is modeled on Germany's Industrie 4.0 plan. In the context of this competition, German experts suggest that China has conducted industrial espionage against the country's car manufacturing, renewable energy, chemistry, communications, optics, x-ray technology, machinery, materials research, and armaments industries.[101] In just one month, a single German telecommunications firm reported over 30,000 Chinese cyber attacks.[102] Estimates indicate that German firms lose $28-71 billion annually as a result.[103] Several cases of Chinese espionage have reached German courts, yet most incidents do not even reach the press because companies do not wish to disclose their vulnerabilities

97. Office of the United States Trade Representative, "Initiation of Section 301 Investigation; Hearing; and Request for Public Comments: China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation," August 18, 2017. (https://ustr.gov/sites/default/files/301/FRN%20China%20301.pdf); See also: Elizabeth Dwoskin, "While Trump fights over aluminum and steel, Silicon Valley braces for a real trade war," *The Washington Post*, March 9, 2018. (https://www.washingtonpost.com/business/economy/while-trump-fights-over-aluminum-and-steel-silicon-valley-braces-for-a-real-trade-war/2018/03/09/95a5446c-6078-45d0-87d5-8838a2638e45_story.html?utm_term=.50116207fcc1)

98. Office of the United States Trade Representative, "2018 Special 301 Report," April 3, 2018, page 1. (https://ustr.gov/sites/default/files/files/Press/Reports/2018%20Special%20301.pdf)

99. Office of the United States Trade Representative, "Findings of the Investigation into China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation Under Section 301 of the Trade Act of 1974," March 22, 2018. (https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF)

100. Office of the Director of National Intelligence, Office of the National Counterintelligence Executive, "Foreign Spies Stealing US Economic Secrets in Cyberspace," October 2011, pages B-1-B-2. (https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/20111103_report_fecie.pdf)

101. Kate Connolly, "Germany accuses China of industrial espionage," *The Guardian* (UK), July 22, 2009. (http://www.theguardian.com/world/2009/jul/22/germany-china-industrial-espionage)

102. William Wilkes, "Hit by Chinese Hackers Seeking Industrial Secrets, German Manufacturers Play Defense," *The Wall Street Journal*, September 23, 2017. (https://www.wsj.com/articles/hit-by-chinese-hackers-seeking-industrial-secrets-german-manufacturers-play-defense-1506164404)

103. Office of the Director of National Intelligence, Office of the National Counterintelligence Executive, "Foreign Spies Stealing US Economic Secrets in Cyberspace," October 2011, page B-1. (https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/20111103_report_fecie.pdf)

or risk business opportunities in China.[104] In 2017, the German government began to take more aggressive defensive steps, including publicly stating that a Chinese hacking group was behind intrusions against high-technology German firms.

Quantitative assessments of the economic harm from intellectual property infringement typically include its effects on industry, consumers, lost tax revenue, and the broader economy.[105] In 2011, a U.S. Commerce Department study found that intellectual property theft costs American companies between $200 and $250 billion per year.[106] Another 2011 report concluded that if Chinese protection of intellectual property matched that of the United States, then the U.S. economy would gain $107 billion in sales and 2.1 million jobs.[107] A 2014 estimate suggests a U.S. loss of $180 to $540 billion due to trade secret theft, although not all of these losses are due to cyber-enabled activities.[108]

Perhaps the most often cited figure comes from the Commission on the Theft of American Intellectual Property (the IP Commission), which concluded that U.S. losses from intellectual property theft amount to over $300 billion per year, with China accounting for roughly 70 percent of those losses (but varying substantially depending on the industry).[109] In a 2017 update to its original 2013 report, the Commission suggested "a low-end estimate of the cost of IP theft" exceeds $225 billion and could be as high as $600 billion.[110]

Most quantitative estimates of damage typically attempt to evaluate the volume or dollar value of illicit goods seized, estimate the ratio of licit to illicit goods, or use extrapolations based on consumer surveys. Yet these approaches often ignore the second-order effects, such as intellectual property protection costs and discouraged investments. With nearly 20 percent of U.S. jobs in intellectual property-intensive industries, the magnitude of the challenge is substantial.[111]

Sustained intellectual property theft has adverse long-term consequences on targeted countries and firms. Stolen intellectual property often enables competitors to enter markets and capture market

104. Kate Connolly, "Germany accuses China of industrial espionage," *The Guardian* (UK), July 22, 2009. (http://www.theguardian.com/world/2009/jul/22/germany-china-industrial-espionage)

105. An important distinction in the following calculations is between economic espionage and trade secret theft according to the 1996 Economic Espionage Act. Economic espionage requires "intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent." Economic espionage is done for the benefit of a foreign nation, whereas theft of trade secrets is done for the economic benefit of an individual or organization. The Economic Espionage Act is extraterritorial; it applies as long as an act in furtherance of the offense was committed in the United States or was conducted by a U.S. individual or organization. See: Economic Espionage, 18 U.S. Code § 1831. (https://www.law.cornell.edu/uscode/text/18/1831)

106. U.S. Department of Commerce "Stolen Intellectual Property Harms American Businesses Says Acting Deputy Secretary Blank," November 29, 2011.

107. U.S. International Trade Commission, "China: Effects of Intellectual Property Infringement and Indigenous Innovation Policies on the U.S. Economy," May 2011, pages xviii–xx. (http://www.usitc.gov/publications/332/pub4226.pdf)

108. "Economic Impact of Trade Secret Theft: A Framework for Companies to Safeguard Trade Secrets and Mitigate Potential Threats," *Center for Responsible Enterprise and Trade and PricewaterhouseCoopers*, February 2014. (https://create.org/resource/economic-impact-of-trade-secret-theft/)

109. Dennis C. Blair and Jon M. Huntsman, Jr., "The Report of the Commission on the Theft of American Intellectual Property," *National Bureau of Asian Research*, May 2013, page 3. (http://ipcommission.org/report/IP_Commission_Report_052213.pdf)

110. Dennis C. Blair and Jon M. Huntsman, Jr., "The Theft of American Intellectual Property: Reassessments of the Challenge and United States Policy," Update to the IP Commission Report, *National Bureau of Asian Research*, February 27, 2017, page 7. (http://www.ipcommission.org/report/IP_Commission_Report_Update_2017.pdf)

111. U.S. Department of Commerce, U.S. Patent and Trademark Office, "Intellectual Property and the U.S. Economy: Industries in Focus," March 2012. (https://www.uspto.gov/sites/default/files/news/publications/IP_Report_March_2012.pdf)

share more quickly and cheaply than they could have done otherwise.[112] In addition, there are substantial costs incurred to investigate theft, counter its impact on brand and reputation, and install additional protection to prevent further leakage. Reduced profits may also decrease reinvestment in equipment and marketing, as well as research and development. Decreased revenues and profits may also raise the cost of obtaining capital, further damaging competitiveness. Reduced investment also has spillover consequences, decreasing the ability to produce leading-edge innovations. Systemic intellectual property theft degrades entrepreneurial motivation when startups cannot leverage their intellectual property to secure financing.[113]

Such adverse effects can damage national competitiveness in certain industries and sectors.[114] For U.S. policymakers, the issue of intellectual property theft is not just a matter of commercial competition but of Washington's ability to rely on its defense industrial base and economy writ large to support U.S. national security.

Critical Infrastructure Intrusions

The Defense Science Board has warned that "for at least the next decade, the offensive cyber capabilities of our most capable adversaries are likely to far exceed the United States' ability to defend key critical infrastructures. The U.S. military itself has a deep and extensive dependence on information technology as well, creating a massive attack surface."[115] As President Obama further explained, "Taking down vital banking systems could trigger a financial crisis. The lack of clean water or functioning hospitals could spark a public health emergency. And as we've seen in past blackouts, the loss of electricity can bring businesses, cities and entire regions to a standstill."[116] Furthermore, Cisco systems has warned that "some adversaries now have the ability – and often now, it seems, the inclination – to lock systems and destroy data as part of their attack process. …[O]ur researchers see this more sinister activity as a precursor to a new and devastating type of attack that is likely to emerge in the near future: Destruction of service (DeOS)."[117] This capability has the potential to make cyber intrusions much more devastating.

112. China often forces foreign companies to divulge source code, use Chinese networks, and comply with new data protection laws as a prerequisites for operating in China. These measures potentially leave companies and their information vulnerable to Chinese intrusions. For example, see: Office of the Director of National Intelligence, National Counterintelligence and Security Center, "Foreign Economic Espionage in Cyberspace," July 26, 2018, pages 13-14. (https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf)

113. Samantha Ravich, "State-Sponsored Cyberspace Threats: Recent Incidents and U.S. Policy Response," *Testimony before the Senate Foreign Relations Subcommittee on East Asia, the Pacific, and International Cybersecurity*, June 13, 2017. (http://www.defenddemocracy.org/content/uploads/documents/6132017_Ravich_Testimony.pdf)

114. For discussions of the adverse consequences of China's IP theft campaigns, see: Dennis C. Blair and Jon M. Huntsman, Jr., "The Theft of American Intellectual Property: Reassessments of the Challenge and United States Policy," Update to the IP Commission Report, *National Bureau of Asian Research*, February 27, 2017, page 7. (http://www.ipcommission.org/report/IP_Commission_Report_Update_2017.pdf); United States International Trade Commission, "China: Effects of Intellectual Property Infringement and Indigenous Innovation Policies on the U.S. Economy," May 2011. (https://www.usitc.gov/publications/332/pub4226.pdf); U.S. Congress Joint Economic Committee Chairman's Staff, "The Impact of Intellectual Property Theft on the Economy," August 2012. (https://www.jec.senate.gov/public/_cache/files/aa0183d4-8ad9-488f-9e38-7150a3bb62be/intellectual-property-theft-and-the-economy.pdf); John Gelinne, J. Donald Fancher, and Emily Mossburg, "The hidden costs of an IP breach: Cyber theft and the loss of intellectual property," *Deloitte*, July 25, 2016. (https://www2.deloitte.com/insights/us/en/deloitte-review/issue-19/loss-of-intellectual-property-ip-breach.html)

115. U.S. Department of Defense, Defense Science Board, "Task Force on Cyber Deterrence," February 2017, Memorandum for the Chairman. (https://www.acq.osd.mil/dsb/reports/2010s/DSB-CyberDeterrenceReport_02-28-17_Final.pdf)

116. Barack Obama, "Taking the Cyberattack Threat Seriously," *The Wall Street Journal*, July 19, 2012. (https://www.wsj.com/articles/SB10000872396390444330904577535492693044650)

117. "Cisco 2017 Midyear Cybersecurity Report," *Cisco Systems*, July 2017, page 3. (https://www.automation.com/pdf_articles/cisco/Cisco_2017_MCR_Embargoed_til_072017_5_AM_PT_8_AM_ET.pdf)

China has reportedly compromised the U.S. power grid and planted backdoors that could be used in a conflict, according to former director of the National Security Agency Admiral Michael Rogers.[118] Numerous U.S. agencies and officials have warned of this and other similar threats.[119] The ability to disrupt U.S. critical infrastructure could trigger a panic, and therefore provide China with the ability to deter U.S. military action against China in the event of a serious provocation. Moreover, this type of cyber attack could degrade Washington's ability to mobilize its military. Chinese cyber operations against the U.S. homeland might be one of the PLA's most attractive military options in a major conflict.

"The ability to disrupt U.S. critical infrastructure could trigger a panic, and therefore provide China with the ability to deter U.S. military action against China in the event of a serious provocation. Moreover, this type of cyber attack could degrade Washington's ability to mobilize its military."

China might also utilize computer network attack capabilities to "attack select nodes on the military's Non-classified Internet Protocol Router Network (NIPRNET) and unclassified DoD and civilian contractor logistics networks in the continental U.S. (CONUS) and allied countries in the Asia-Pacific region."[120] Chinese government sources have even publicly acknowledged elements of this approach, with the *People's Daily* noting that U.S. reliance on networks will "leave the country more vulnerable and turn out to be the lower-hanging fruit in the face of cyber attacks."[121] In wartime, it might prove difficult to intrude into many classified U.S. networks, but the sensitive yet often unclassified networks that handle logistics data for the U.S. military would prove tempting targets.

A reliance on equipment produced by Chinese enterprises may be a leading cause of vulnerability for U.S. supply chains and critical infrastructure.[122] In particular, there are concerns that some Chinese technology products, such as network routers, could facilitate illicit access to U.S. critical infrastructure.[123] For example, a 2016 Pentagon report warned that Lenovo systems might pose a cyber espionage risk to Defense Department supply chains, and some had been found to communicate information back to Chinese intelligence.[124] Chinese technology companies Huawei

118. Ken Dilanian, "NSA director: China can damage US power grid," *Associated Press*, November 20, 2014. (https://apnews.com/cb45fcf4e9c9453d8fb0098e445ae425)

119. For example, see: U.S.-China Economic and Security Review Commission, "2009 Annual Report to Congress," November 1, 2009, page 167-183. (https://www.uscc.gov/Annual_Reports/2009-annual-report-congress)

120. Bryan Krekel, "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation," *U.S.-China Economic and Security Review Commission*, October 9, 2009, page 8. (https://nsarchive2.gwu.edu//NSAEBB/NSAEBB424/docs/Cyber-030.pdf)

121. "Double-edged sword: US simulated cyber-attack," *People's Daily* (China), March 18, 2008. (http://english.peopledaily.com.cn/90001/90780/91343/6375863.html)

122. For additional information on supply chain vulnerabilities, see: Tara Beeny, "Supply Chain Vulnerabilities from China in U.S. Federal Information and Communications Technology," *U.S.-China Economic and Security Review Commission*, April 2018. (https://www.uscc.gov/sites/default/files/Research/Interos_Supply%20Chain%20Vulnerabilities%20from%20China%20in%20U.S.%20Federal%20ICT_final.pdf)

123. For example, see: Darren Allan, "Dangerous backdoor exploit found on popular IoT devices," *TechRadar*, March 2, 2017. (https://www.techradar.com/news/dangerous-backdoor-exploit-found-on-popular-iot-devices)

124. Hayley Tsukayama and Dan Lamothe, "How an email sparked a squabble over Chinese-owned Lenovo's role at Pentagon," *The Washington Post*, April 22, 2016. (https://www.washingtonpost.com/business/economy/how-an-email-sparked-a-squabble-over-chinese-owned-lenovos-role-at-pentagon/2016/04/22/b1cd43d8-07ca-11e6-a12f-ea5aed7958dc_story.html)

and ZTE have drawn substantial attention for being "financially and politically supported by the Chinese government."[125] Chinese companies deny that the government uses their products for computer network exploitations, but U.S. researchers have found that "risks associated with Huawei's and ZTE's provision of equipment to U.S. critical infrastructure could undermine core U.S. national-security interests."[126] A 2013 UK parliamentary committee similarly raised concerns about Huawei's position within British critical national infrastructure.[127] In April 2018, the UK's National Cyber Security Centre warned private telecommunications companies against working with ZTE because coupling ZTE and Huawei products would create "an unacceptable national security risk" and render "existing [threat] mitigations ineffective."[128]

"The PRC has integrated cyber intrusions into the suite of tools it uses to pressure foreign governments and corporations to reverse unfavorable decisions. In a notable example last year, China employed economic sanctions and cyber operations to pressure the South Korean government to stop deployment of the U.S. THAAD missile defense system."

Cyber-Enabled Economic Coercion

The PRC has integrated cyber intrusions into the suite of tools it uses to pressure foreign governments and corporations to reverse unfavorable decisions. In a notable example last year, China employed economic sanctions and cyber operations to pressure the South Korean government to stop deployment of the U.S. THAAD missile defense system.[129] Beijing specifically targeted Lotte Group, a South Korean conglomerate that agreed to allow the Korean government to use a golf course for the deployment of THAAD. Lotte initially faced a cyber attack from Chinese internet protocol addresses that took parts

125. Bruce Gilley, "Huawei's Fixed Line to Beijing," *Far Eastern Economic Review*, January 4, 2001, page 94. (http://www.web.pdx.edu/~gilleyb/Huawei_FEER28Dec2000.pdf)

126. A 2012 investigation also found that Huawei "exhibits a pattern of disregard for the intellectual property rights" of other companies. The most notable case involved the sale by Huawei of products using Cisco's patented technology. Cisco sued Huawei in 2003, accusing the company of accessing Cisco's code, electronically copying it, and inserting it into its own products. In another case, Canadian telecom company Nortel suffered significant breaches by Chinese cyber actors. After the company declared bankruptcy, its former security advisor accused the hackers of working "on behalf of Huawei and ZTE and other Chinese companies." See: House Permanent Select Committee on Intelligence, "Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE," October 8, 2012, page 31. (https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20(final).pdf); Mark Chandler, "Huawei and Cisco's Source Code: Correcting the Record," *Cisco Blogs*, October 11, 2012. (https://blogs.cisco.com/news/huawei-and-ciscos-source-code-correcting-the-record); John Kehoe, "How Chinese hacking felled telecommunication giant Nortel," *The Australian Financial Review*, May 26, 2014. (http://www.afr.com/technology/web/security/how-chinese-hacking-felled-telecommunication-giant-nortel-20140526-iux6a); Laura Payton, "Former Nortel exec warns against working with Huawei," *CBC News*, October 11, 2012. (https://www.cbc.ca/news/politics/former-nortel-exec-warns-against-working-with-huawei-1.1137006)

127. UK Parliament, Intelligence and Security Committee, "Foreign involvement in the Critical National Infrastructure: The implications for national security," June 2013. (https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20130606_ISC_CNI_Report.pdf?attachauth=ANoY7crPKAthnGYmvx4Po16NbvAmCOkFPTzhJHUxqeYgh-ZgqIptVZ-doApV_WWasJF-6QXgVsXzUorm58owG9lehniC74YzTqUIyWRYa8kmwyVctVRb6JrkJ9kHh1dNc-rASg4RvxacLHXZSoHgiRoRsMKQcJHuOypasKhKCKWkq0oV1uBkGECL3dk-0ch1xg-126zGP4Is8tyapVHuCBkX8KwVto05mc6jXUctspw5I4HjSCp4g-c%3D&attredirects=2)

128. Nic Fildes, "Cyber security watchdog warns UK telcos against using equipment from Chinese supplier ZTE," *The Financial Times* (UK), April 16, 2018. (https://www.ft.com/content/24c998b4-416c-11e8-803a-295c97e6fd0b)

129. In previous incidents, China banned South Korean cells phones and plastics from Chinese markets when the two countries were in a dispute over Chinese garlic exports to South Korea. Don Kirk and International Herald Tribune, "Just a Little Garlic Overpowers Asian Trade Ties," *The New York Times*, July 8, 2000. (https://www.nytimes.com/2000/07/08/news/just-a-little-garlic-overpowers-asian-trade-ties.html); Bonnie S. Glaser, Daniel G. Sofio, and David A. Parker, "The Good, the THAAD, and the Ugly," *Foreign Affairs*, February 15, 2017. (https://www.foreignaffairs.com/articles/united-states/2017-02-15/good-thaad-and-ugly)

of its storefront offline for several days.[130] In the first half of 2017, attempted cyber intrusions emanating from China against South Korean Foreign Ministry servers increased to more than 6,000 as compared to about 4,600 during all of 2016.[131]

"The U.S. government has asserted that Chinese groups have infiltrated the networks of numerous companies and institutions not only in the United States but around the world. Since 2015, the U.S. intelligence community assesses that most detected Chinese cyber operations have been focused on defense, technology, and communications companies whose products are widely used in the public and private sectors."

In addition to the cyber attacks against Lotte, some Chinese e-commerce sites stopped cooperating with the South Korean company. Afterwards, the Chinese government shuttered nearly all of Lotte's 115 physical stores in China, citing fire risks and other pretexts.[132] Chinese media also called for boycotts of South Korean goods and a ban on travel to South Korea.[133] The Chinese tourism ministry reportedly instructed tour operators to stop selling trips to South Korea.[134] The incident reportedly shaved 0.4 percent from South Korea's gross domestic product,[135] providing a lesson to other countries that China can use coercive and cyber-enabled economic measures to shape their foreign policy.

Examples of Chinese Cyber-Enabled Intrusions

The U.S. government has asserted that Chinese groups have infiltrated the networks of numerous companies and institutions not only in the United States but around the world. Since 2015, the U.S. intelligence community assesses that most detected Chinese cyber operations have been focused on defense, technology, and communications companies whose products are widely used in the public and private sectors.[136] To date, however, there remains no central repository of this data. Many companies remain hesitant to share information about exploitations, but enough information is now available to demonstrate the types of intrusions that are typical of Chinese hackers.

The following chart contains examples of Chinese cyber intrusions conducted against firms in the United States and its allies and partners, as well as a number of government institutions. The cases included illustrate the types of attacks China undertakes, but it is not an exhaustive list.

130. Simon Atkinson, "Is China retaliating against Lotte missile deal?" *BBC News* (UK), March 6, 2017. (http://www.bbc.com/news/business-39176388)
131. "Cyberattack Attempts from China on S. Korean Foreign Ministry Surge This Year," *KBS Radio*, September 10, 2017. (http://world.kbs.co.kr/service/news_view.htm?lang=e&Seq_Code=130047)
132. Joyce Lee and Adam Jourdan, "South Korea's Lotte reports store closures in China amid political stand-off," *Reuters*, March 6, 2017. (https://www.reuters.com/article/us-southkorea-china-lotte/south-koreas-lotte-says-four-retail-stores-in-china-closed-after-inspections-idUSKBN16D03U)
133. William Ide, "Chinese Media Call for Boycott of South Korean Goods," *Voice of America*, March 2, 2017. (https://www.voanews.com/a/chinese-media-call-for-boycott-of-south-korean-goods/3746701.html)
134. Joyce Lee and Adam Jourdan, "South Korea's Lotte reports store closures in China amid political stand-off," *Reuters*, March 6, 2017. (https://www.reuters.com/article/us-southkorea-china-lotte/south-koreas-lotte-says-four-retail-stores-in-china-closed-after-inspections-idUSKBN16D03U)
135. Kanga Kong and Jiyeun Lee, "China, South Korea Agree to Shelve Thaad Missile Shield Spat," *Bloomberg*, October 31, 2017. (https://www.bloomberg.com/news/articles/2017-10-31/china-south-korea-agree-to-shelve-thaad-missile-shield-dispute)
136. Office of the Director of National Intelligence, National Counterintelligence and Security Center, "Foreign Economic Espionage in Cyberspace," July 26, 2018, page 7. (https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf)

YEAR	TARGET	SECTOR	DETAILS
2006	**Ford**	**Automotive**	Xu Xiang Dong, a product engineer at Ford, copied 4,000 documents onto an external hard drive in an effort to obtain a job at a Chinese automotive company.[137] Ford's loss was estimated at $50 million.[138]
2007	**QinetiQ**	**Robotics**	QinetiQ suffered an intrusion that gave hackers access to information on robotics, satellites, combat helicopters, and unmanned aerial vehicles.[139] The PLA later displayed a bomb disposal robot that likely reflected stolen QinetiQ technology.[140]
2008	**Alcoa**	**Metals**	A breach at Alcoa enabled hackers to access emails containing internal discussions about a potential deal with a Chinese state-owned enterprise.[141]
2009	**Coca-Cola**	**Beverage**	Coca-Cola suffered an intrusion by the Comment Crew (likely PLA Unit 61398) permitting access to Coca-Cola's corporate network while the firm attempted to acquire China Huiyuan Juice Group.[142]
2009	**Valspar**	**Chemical**	David Yen Lee, an employee of Valspar Corporation, downloaded the proprietary paint formulas for 160 products, valued at $20 million and equal to one-eighth of Valspar's yearly profits. He intended to provide this information for a new job in Shanghai at Nippon Paint.[143] The trade secrets were valued at $7 to $20 million.[144]

137. Office of the Director of National Intelligence, Office of the National Counterintelligence Executive, "Foreign Spies Stealing US Economic Secrets in Cyberspace," October 2011, page 4. (https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/20111103_report_fecie.pdf)
138. Executive Office of the President of the United States, "Administration Strategy on Mitigating the Theft of U.S. Trade Secrets," February 2013, page 4. (https://committee100.org/wp-content/uploads/2017/07/nps49-022113-01.pdf)
139. Larry M. Wortzel, "Cyber Espionage and the Theft of U.S. Intellectual Property and Technology," Testimony before *the House Energy and Commerce Subcommittee on Oversight and Investigations, July 9, 2013. (*http://docs.house.gov/meetings/IF/IF02/20130709/101104/HHRG-113-IF02-Wstate-WortzelL-20130709-U1.pdf)
140. See: Jonathan Ray, Katie Atha, Edward Francis, Caleb Dependahl, James Mulvenon, Daniel Alderman, and Leigh Ann Ragland-Luce, "China's Industrial and Military Robotics Development," U.S.-China Economi*c and Security Review Commission, October 2016. (*https://www.uscc.gov/sites/default/files/Research/DGI_China%27s%20Industrial%20and%20Military%20Robotics%20Development.pdf); Michael Riley and Ben Elgin, "China's Cyberspies Outwit Model for Bond's Q," Bloomberg, May 2*, 2013. (*https://www.bloomberg.com/news/articles/2013-05-01/china-cyberspies-outwit-u-s-stealing-military-secrets)
141. Jim Finkle, Joseph Menn, Aruna Viswanatha, "U.S. accuses China of cyber spying on American companies," Reuters, November 20, *2014. (*https://www.reuters.com/article/us-cybercrime-usa-china/u-s-accuses-china-of-cyber-spying-on-american-companies-idUSKCN0J42M520141120); U.S. Department of Justice, Press Release, "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage," May 19, 2014. (https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor)
142. David E. Sanger, David Barboza, and Nicole Perlroth, "China's Army Is Seen as Tied to Hacking Against U.S.," The New York Times, Fe*bruary 18, 2013. (*http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html)
143. Office of the Director of National Intelligence, Office of the National Counterintelligence Executive, "Foreign Spies Stealing US Economic Secrets in Cyberspace," October 2011, page 3. (https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/20111103_report_fecie.pdf)
144. Executive Office of the President of the United States, "Administration Strategy on Mitigating the Theft of U.S. Trade Secrets," February 2013, page 9. (https://committee100.org/wp-content/uploads/2017/07/nps49-022113-01.pdf)

YEAR	TARGET	SECTOR	DETAILS
2009	**DuPont**	**Chemicals**	Meng Hong, a research chemist at DuPont Corporation, downloaded proprietary information on organic light-emitting diodes and intended to provide the information to commercialize the product while at Peking University.[145] The firm's loss was estimated at $400 million.[146]
2010	**Google**	**Technology**	Operation Auroru targeted 34 companies in the technology, finance, and defense sectors, including Google.[147] Google suffered intrusions going after human rights activists and dissidents.[148] Google suggested that Chinese actors had stolen its source code.[149]
2010	**Various**	**Aviation**	Dongfan Chung was sentenced to 15 years in prison for economic espionage on behalf of the Chinese aviation industry. He had 250,000 pages of sensitive documents in his house.[150]
2010	**Various**	**Communications**	U.S. internet traffic was re-routed through China for 18 minutes, permitting Chinese groups to monitor 15 percent of global traffic.[151]
2010	**U.S. Steel**	**Metals**	U.S. Steel computers were exploited, starting in 2010, while U.S. Steel pursued trade cases against Chinese steel companies.[152] U.S. Steel alleges that Chinese hackers stole proprietary methods for producing lightweight steel to advantage Chinese steel producers.
2010	**Westinghouse**	**Nuclear**	Attackers stole from Westinghouse the specifications for pipes, supports, and routing in its AP1000 power plants, as well as emails related to Westinghouse's business with a Chinese state-owned enterprise.[153]

145. Office of the Director of National Intelligence, Office of the National Counterintelligence Executive, "Foreign Spies Stealing US Economic Secrets in Cyberspace," October 2011, page 3. (https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/20111103_report_fecie.pdf)
146. Executive Office of the President of the United States, "Administration Strategy on Mitigating the Theft of U.S. Trade Secrets," February 2013, page 5. (https://committee100.org/wp-content/uploads/2017/07/nps49-022113-01.pdf)
147. Kim Zetter, "Google Hack Attack was Ultra Sophisticated, New Details Show," Wired, January 14, 20*10. (*https://www.wired.com/2010/01/operation-aurora/)
148. Ellen Nakashima, "U.S. said to be target of massive cyber-espionage campaign," The Washington Post, F*ebruary 10, 2013. (*https://www.washingtonpost.com/world/national-security/us-said-to-be-target-of-massive-cyber-espionage-campaign/2013/02/10/7b4687d8-6fc1-11e2-aa58-243de81040ba_story.html)
149. Office of the Director of National Intelligence, Office of the National Counterintelligence Executive, "Foreign Spies Stealing US Economic Secrets in Cyberspace," October 2011, page 5. (https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/20111103_report_fecie.pdf)
150. Ibid, page 2.
151. Caroline Alphonso, "China's 'hijacking' of U.S. data flow stokes fear of cyberespionage," The Globe and Mail (Canada), No*vember 18, 2010. (*https://www.theglobeandmail.com/technology/chinas-hijacking-of-us-data-flow-stokes-fear-of-cyberespionage/article1314598/)
152. John W. Miller, "U.S. Steel Accuses China of Hacking," The Wall Street Jou*rnal, April 28, 2016. (*https://www.wsj.com/articles/u-s-steel-accuses-china-of-hacking-1461859201); U.S. Department of Justice, Press Release, "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage," May 19, 2014. (https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor)
153. Anya Litvak, "Westinghouse's data stolen despite big deal with China," Pittsburgh Post-G*azette, May 19, 2014. (*http://www.post-gazette.com/local/city/2014/05/20/Westinghouse-s-data-stolen-despite-big-deal-with-China/stories/201405200086); U.S. Department of Justice, Press Release, "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage," May 19, 2014. (https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor)

YEAR	TARGET	SECTOR	DETAILS
2011	**RSA**	**Defense**	RSA suffered an attack by three Chinese groups that led to later intrusions that compromised security in 20 percent of Fortune 100 companies. Estimates suggest that 720 companies were affected, including defense firms such as Lockheed Martin.[154]
2011	**Various**	**Energy**	McAfee released information on "Night Dragon" showing that intruders had exfiltrated data from oil, energy, and petrochemical companies to an IP address in China.[155]
2011	**Cargill**	**Agriculture**	A former employee of both Cargill and Dow Chemical was convicted of providing trade secrets on organic pesticides to a Chinese university. Financial losses exceeded $7 million.[156]
2011	**Motorola**	**Electronics**	A Motorola software engineer attempted to hand over stolen trade secrets – including 1,000 sensitive Motorola documents – on mobile telecommunications to the Chinese military.[157] The proprietary data was estimated at $600 million.[158]
2011	**American Superconductor Corporation (AMSC)**	**Electronics**	American Superconductor suffered an intrusion that resulted in the disclosure of its source code to Sinovel.[159] In January 2018, Sinovel was convicted of stealing trade secrets in order to copy AMSC's technology and products. As a result of the IP theft, AMSC suffered "devastating harm," and Sinoval's actions "nearly destroyed" AMSC, according to the U.S. Justice Department.[160]
2012	**SolarWorld**	**Energy**	SolarWorld saw files stolen that contained information about its cash flow, manufacturing metrics, production line information, costs, and trade litigation. Around the same time, Chinese firms dumped solar products into U.S. markets.[161]

154. David E. Sanger, David Barboza, and Nicole Perlroth, "China's Army Is Seen as Tied to Hacking Against U.S.," The New York Times, Fe*bruary 18, 2013. (*http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html); Brian Krebs, "Who Else Was Hit by the RSA Attackers?" Krebs on Security*, October 2011. (*https://krebsonsecurity.com/2011/10/who-else-was-hit-by-the-rsa-attackers/)

155. "China-based hackers targeted oil, energy companies in 'Night Dragon' cyber attacks, McAfee says," Los Angeles Times, Feb*ruary 10, 2011. (*http://latimesblogs.latimes.com/technology/2011/02/chinese-hackers-targeted-oil-companies-in-cyberattack-mcafee-says.html)

156. Executive Office of the President of the United States, "Administration Strategy on Mitigating the Theft of U.S. Trade Secrets," February 2013, page 7. (https://committee100.org/wp-content/uploads/2017/07/nps49-022113-01.pdf)

157. Ibid, page 10.

158. Ellen Nakashima, "In a world of cybertheft, U.S. names China, Russia as main culprits," The Washington Post, *November 3, 2011. (*https://www.washingtonpost.com/world/national-security/us-cyber-espionage-report-names-china-and-russia-as-main-culprits/2011/11/02/gIQAF5fRiM_story.html)

159. Larry M. Wortzel, "Cyber Espionage and the Theft of U.S. Intellectual Property and Technology," Testimony before *the House Energy and Commerce Subcommittee on Oversight and Investigations, July 9, 2013. (*http://docs.house.gov/meetings/IF/IF02/20130709/101104/HHRG-113-IF02-Wstate-WortzelL-20130709-U1.pdf)

160. U.S. Department of Justice, Press Release, "Chinese Company Sinovel Wind Group Convicted of Theft of Trade Secrets," January 24, 2018. (https://www.justice.gov/opa/pr/chinese-company-sinovel-wind-group-convicted-theft-trade-secrets)

161. Everett Rosenfeld, "Solar company takes on China—and US rivals," CNBC, May 21, 201*4. (*https://www.cnbc.com/2014/05/21/solarworld-vs-china-one-companys-war-with-china-may-have-gotten-them-hacked.html)

YEAR	TARGET	SECTOR	DETAILS
2012	**Allegheny Technologies**	**Communications**	Allegheny Technologies suffered an intrusion that compromised the network credentials of nearly all its employees. The intrusion occurred during trade disputes with a Chinese state-owned enterprise.[162]
2012	**United Steel Workers**	**Metals**	United Steel Workers' emails containing information about its strategies in trade disputes and related legislative proposals were stolen.[163]
2012	**NASA**	**Aerospace**	NASA disclosed that it had suffered an attack that gave the intruders full network control, which could have potentially led to Chinese advances in aerospace technologies.[164]
2012	**Telvent**	**Energy**	Telvent Canada suffered an intrusion that may have compromised many of the oil and gas pipelines and power grids in North America.[165]
2012	**Multiple**	**Various**	Operation Shady RAT targeted 21 government entities, 13 defense contractors, 13 technology firms, 6 industrial groups, and a handful of non-profit organizations.[166] Most of the targets were in the United States, but others included groups in Canada, Taiwan, Japan, South Korea, the United Kingdom, and elsewhere.
2012	**General Motors**	**Automotive**	A jury found two individuals guilty of attempting to steal General Motors' trade secrets on hybrid vehicle technology and provide the information to a competing Chinese automotive company. The technology was estimated to be worth $40 million.[167]
2012	**U.S. Transportation Command**	**Industrial Base**	Chinese hackers gained access to the U.S. Transportation Command, conducting at least 20 intrusions into the U.S. military's logistics and supply systems through defense contractors.[168]

162. David Kravets, "How China's army hacked America," Ars Technica, May *19, 2014. (*https://arstechnica.com/tech-policy/2014/05/how-chinas-army-hacked-american-companies/)
163. Leo W. Gerard, "Outlaw Chinese Steel," United Steelwork*ers, May 3, 2016. (*https://www.usw.org/blog/2016/outlaw-chinese-steel); U.S. Department of Justice, Press Release, "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage," May 19, 2014. (https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor)
164. Larry M. Wortzel, "Cyber Espionage and the Theft of U.S. Intellectual Property and Technology," Testimony before *the House Energy and Commerce Subcommittee on Oversight and Investigations, July 9, 2013. (*http://docs.house.gov/meetings/IF/IF02/20130709/101104/HHRG-113-IF02-Wstate-WortzelL-20130709-U1.pdf)
165. David E. Sanger, David Barboza, and Nicole Perlroth, "China's Army Is Seen as Tied to Hacking Against U.S.," The New York Times, F*ebruary 18, 2013. (*http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html); See also: Brian Krebs, "Chinese Hackers Blamed for Intrusion at Energy Industry Giant Telvent," Kre*bs on Security, (*https://krebsonsecurity.com/2012/09/chinese-hackers-blamed-for-intrusion-at-energy-industry-giant-telvent/)
166. Dmitri Alperovitch, "Revealed: Operation Shady RAT," McAfee, August 2012, pag*e 4. (*http://www.csri.info/wp-content/uploads/2012/08/wp-operation-shady-rat1.pdf)
167. Executive Office of the President of the United States, "Administration Strategy on Mitigating the Theft of U.S. Trade Secrets," February 2013, page 7. (https://committee100.org/wp-content/uploads/2017/07/nps49-022113-01.pdf)
168. Senate Armed Services Committee, Press Release, "SASC investigation finds Chinese intrusions into key defense contractors," September 17, 2014. (https://www.armed-services.senate.gov/press-releases/sasc-investigation-finds-chinese-intrusions-into-key-defense-contractors)

YEAR	TARGET	SECTOR	DETAILS
2013	**National Electrical Manufacturers Association**	**Energy**	The National Electrical Manufacturers Association was the target of a failed attack by APT1 (likely PLA Unit 61398).[169]
2013	**New York Times and Wall Street Journal**	**Media**	Hackers based in China targeted the *New York Times* and the *Wall Street Journal* computer systems, likely in response to reporting about the finances of Wen Jiabao's family.[170]
2013	**Multiple**	**Aerospace**	Chinese hackers attempted to access designs and technologies related to unmanned aerial vehicles, with 123 attacks targeting U.S. companies.[171]
2014	**Community Health Systems**	**Healthcare**	In 2014, Chinese hackers compromised Community Health Systems' networks, resulting in the theft of social security numbers and other personal information of 4.5 million individuals.[172]
2014	**Siemens**	**Industrial manufacturing**	A Chinese national allegedly accessed Siemens's networks in 2014 and stole more than 400 gigabytes of proprietary commercial data in 2015.[173]
2014	**Anthem**	**Healthcare**	Health insurance company Anthem was the victim of a data breach, exposing the records of nearly 80 million people.[174] The breach occurred in December 2014 or earlier.[175] Private cybersecurity firm ThreatConnect linked the malware to Chinese state-sponsored actors.[176]

169. David E. Sanger, David Barboza, and Nicole Perlroth, "China's Army Is Seen as Tied to Hacking Against U.S.," The New York Times, F*ebruary 18, 2013. (*http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html)

170. Anna Schecter, "Exclusive: Corporate Victims of Chinese Hackers Speak Out," NBC News, February 22, *2013. (*http://rockcenter.nbcnews.com/_news/2013/02/22/17058583-exclusive-corporate-victims-of-chinese-hackers-speak-out)

171. Alex Pasternack, "Hackers Are Helping China Build Cheap Clones of America's Drones," Motherboard, September *23, 2013. (*https://motherboard.vice.com/en_us/article/mgbqk8/hackers-are-helping-china-build-cheap-clones-of-americas-drones)

172. Jim Finkle and Caroline Humer, "Community Health says data stolen in cyber attack from China," Reuters, August 18, *2014. (*https://www.reuters.com/article/us-community-health-cybersecurity/community-health-systems-says-personal-data-stolen-in-cyber-attack-idUSKBN0GI16N20140818)

173. U.S. Department of Justice, Press Release, "U.S. Charges Three Chinese Hackers Who Work at Internet Security Firm for Hacking Three Corporations for Commercial Advantage," November 27, 2017. (https://www.justice.gov/opa/pr/us-charges-three-chinese-hackers-who-work-internet-security-firm-hacking-three-corporations)

174. Anna Wilde Mathews and Danny Yadron, "Health Insurer Anthem Hit by Hackers," The Wall Street Journ*al, February 4, 2015. (*https://www.wsj.com/articles/health-insurer-anthem-hit-by-hackers-1423103720)

175. Drew Harwell and Ellen Nakashima, "China suspected in major hacking of health insurer," The Washington Post, *February 5, 2015. (*https://www.washingtonpost.com/business/economy/investigators-suspect-china-may-be-responsible-for-hack-of-anthem/2015/02/05/25fbb36e-ad56-11e4-9c91-e9d2f9fde644_story.html?utm_term=.ee63a21737b6)

176. "The Anthem Hack: All Roads Lead to China," ThreatConnect, Februar*y 27, 2015. (*https://www.threatconnect.com/blog/the-anthem-hack-all-roads-lead-to-china/); Ellen Nakashima, "Security firm finds link between China and Anthem hack," The Washington Post, F*ebruary 27, 2015. (*https://www.washingtonpost.com/news/the-switch/wp/2015/02/27/security-firm-finds-link-between-china-and-anthem-hack/?utm_term=.39a985eee0da)

YEAR	TARGET	SECTOR	DETAILS
2015	**Trimble**	**Software**	Chinese nationals allegedly stole 275 megabytes of data from Trimble between December 2015 and March 2016. The Department of Justice noted that the data could assist in the development of competing global navigation systems.[177]
2015	**United Airlines**	**Aviation**	United Airlines detected intrusions in its network possibly carried out by the same Chinese hackers responsible for the Anthem attack and other intrusions.[178]
2016	**Various**	**Semiconductors**	In 2016, three groups based in China compromised the networks of four companies involved in semiconductor manufacturing, according to a FireEye report.[179]
2016	**Various**	**Information Technology**	In "Operation Cloud Hopper," APT10 conducted a sustained cyber campaign against managed IT service providers, accessing intellectual property and sensitive company and customer data.[180]
2017	**Medrobotics Corporation**	**Robotics**	A dual Canadian and Chinese citizen gained physical access to the offices of Medrobotics Corporation and attempted to steal information using a variety of computers and other network equipment.[181] The individual had previously attempted to connect digitally with a number of employees at the firm.
2017	**Multiple**	**Public policy**	Chinese actors conducted cyber espionage against at least six non-governmental organizations. In at least one case, after the intrusion failed, the actor conducted a DDoS attack against the think tank's website.[182]
2018	**Unnamed Contractor**	**Defense**	Chinese government hackers stole sensitive data about a missile project known as Sea Dragon, as well as signals and sensor data and information related to cryptography systems, from a private company working on undersea warfare.[183]

177. U.S. Department of Justice, Press Release, "U.S. Charges Three Chinese Hackers Who Work at Internet Security Firm for Hacking Three Corporations for Commercial Advantage," November 27, 2017. (https://www.justice.gov/opa/pr/us-charges-three-chinese-hackers-who-work-internet-security-firm-hacking-three-corporations)
178. "Hackers with ties to China said to breach United Airlines," Chicago Tribune, *July 29, 2015.* (http://www.chicagotribune.com/business/ct-hackers-breach-united-airlines-20150729-story.html)
179. "Redline Drawn: Cyber Recalculates its Use of Cyber Espionage," FireEye, June 2016, page *13.* (https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf)
180. "Operation Cloud Hopper," PwC UK and BAE *Systems, April 2017.* (https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-report-final-v4.pdf)
181. U.S. Department of Justice, Press Release, "Dual Canadian/Chinese Citizen Arrested for Attempting to Steal Trade Secrets and Computer Information," August 31, 2017. (https://www.justice.gov/usao-ma/pr/dual-canadianchinese-citizen-arrested-attempting-steal-trade-secrets-and-computer)
182. Zaid Shoorbajee, "Chinese hackers tried to spy on U.S. think tanks to steal military strategy documents, CrowdStrike says," CyberScoop, December 2*1, 2017.* (https://www.cyberscoop.com/chinese-hackers-tried-to-spy-on-u-s-think-tanks-to-steal-military-strategy-documents/); Adam Kozy, "An End to 'Smash-and-Grab' and a Move to More Targeted Approaches," CrowdStrike, December *20, 2017.* (https://www.crowdstrike.com/blog/an-end-to-smash-and-grab-more-targeted-approaches/)
183. Ellen Nakashima and Paul Sonne, "China hacked a Navy contractor and secured a trove of highly sensitive data on submarine warfare," The Washington Po*st, June 8, 2018.* (https://www.washingtonpost.com/world/national-security/china-hacked-a-navy-contractor-and-secured-a-trove-of-highly-sensitive-data-on-submarine-warfare/2018/06/08/6cc396fa-68e6-11e8-bea7-c8eb28bc52b1_story.html?noredirect=on&utm_term=.9b12be188d8e)

Overall, the list of incidents above demonstrates the scope and scale of the challenge posed by Chinese groups conducting cyber-enabled economic intrusions. What may not be clear, however, is the serious damage done to many of these companies and the second-order effects on U.S. national security. To that end, it is useful to examine one case in detail: the shift in development and production of solar panels from the United States to China.

As Matthew Stepp and Michelle Wein note, "Beginning in earnest in 2009, artificially cheap Chinese solar products flooded the market and decimated U.S. solar manufacturing. China went from exporting very little solar products to the United States before 2009 to shipping 49 percent of the solar panels deployed in America in 2013. Over 25 U.S. solar manufacturers have gone bankrupt or been forced to lay off workers."[184] During this time, U.S. company SolarWorld claims that Chinese military personnel broke into its systems and stole important business documents related to its trade dispute with China.[185] According to the U.S. Department of Justice, a Chinese hacker named Wen Xinyu reportedly stole emails and files from three executives at SolarWorld that provided Chinese solar panel producers with American and German intellectual property. At the time, SolarWorld was preparing to mass produce Passivated Emitter Rear Contact solar cells.[186] Chinese hackers stole this technology and provided it to Chinese firms, which gained a competitive edge.[187]

Other U.S. firms filed similar cases, including Solaria and Suniya, but at least 30 U.S. solar panel makers went bankrupt as Chinese solar panels flooded world markets.[188] According to one analysis, "The flood of Chinese panels was one of the main reasons why world prices crashed by 80% between 2008 and 2013."[189] The U.S. Trade Representative found that China's share of global solar cell production increased from 7 percent to 61 percent from 2005 to 2012.[190] Today, over 2.5 million people work in China's solar power sector, compared to only 260,000 in the United States.[191]

Although the Trump administration has taken action against Chinese solar panel producers, the U.S. government's ability to protect domestic companies is limited by the rapidity of Chinese exploitation of stolen intellectual property, as well as the difficulty of acquiring sufficient information for the U.S. government to take action against Chinese producers. New policy responses will be necessary to protect U.S. companies, institutions, and individuals against such cyber-enabled economic intrusions.

184. Matthew Stepp and Michelle Wein, "U.S.-China solar trade dispute: Short-term profit vs. long-term viability," *The Hill*, July 24, 2014. (http://thehill.com/blogs/pundits-blog/international/213126-us-china-solar-trade-dispute-short-term-profit-vs-long-term)
185. Sam Frizell, "Here's What Chinese Hackers Actually Stole From U.S. Companies," *Time*, May 20, 2014. (http://time.com/106319/heres-what-chinese-hackers-actually-stole-from-u-s-companies/)
186. Indictment, *United States v. Wang Dong, Sun Kailiang, Wen Xinyu, Huang Zhenyu, and Gu Chunhui*, Criminal No. 14-118 (Western District of Pennsylvania, filed May 1, 2014). (https://www.justice.gov/iso/opa/resources/5122014519132358461949.pdf)
187. Diane Cardwell, "Solar Company Seeks Stiff U.S. Tariffs to Deter Chinese Spying," *The New York Times*, September 1, 2014. (https://www.nytimes.com/2014/09/02/business/trade-duties-urged-as-new-deterrent-against-cybertheft.html); Christian Roselund, "SolarWorld testifies on Chinese IP theft," *PV Magazine*, October 10, 2017. (https://pv-magazine-usa.com/2017/10/10/solarworld-testifies-on-chinese-ip-theft/)
188. Ian Clover, "Solaria files IP lawsuit against GCL over module production infringement," *PV Magazine*, September 28, 2016. (https://www.pv-magazine.com/2016/09/28/solaria-files-ip-lawsuit-against-gcl-over-module-production-infringement_100026283/)
189. Sherisse Pham and Matt Rivers, "China is crushing the U.S. in renewable energy," *CNN*, July 18, 2017. (https://money.cnn.com/2017/07/18/technology/china-us-clean-energy-solar-farm/index.html?iid=EL)
190. Office of the United States Trade Representative, "Findings of the Investigation into China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation Under Section 301 of the Trade Act of 1974," March 22, 2018. (https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF); David J. Lynch, "Trump imposes tariffs on solar panels and washing machines in first major trade action of 2018," *The Washington Post*, January 22, 2018. (https://www.washingtonpost.com/news/wonk/wp/2018/01/22/trump-imposes-tariffs-on-solar-panels-and-washing-machines-in-first-major-trade-action/?utm_term=.e994c5129443)
191. Sherisse Pham and Matt Rivers, "China is crushing the U.S. in renewable energy," *CNN*, July 18, 2017. (https://money.cnn.com/2017/07/18/technology/china-us-clean-energy-solar-farm/index.html?iid=EL)

Policy Responses

Contrary to our hopes, China expanded its power at the expense of the sovereignty of others. China gathers and exploits data on an unrivaled scale and spreads features of its authoritarian system, including corruption and the use of surveillance. It is building the most capable and well-funded military in the world, after our own … Part of China's military modernization and economic expansion is due to its access to the U.S. innovation economy, including America's world-class universities.

- U.S. National Security Strategy (2017)[192]

The Trump administration has made competition with China a central element of its National Security Strategy and National Defense Strategy. Before putting forward specific recommendations on ways to implement Washington's stated goals, however, it is necessary to review recent efforts to alter Chinese behavior.

Lessons from the 2015 U.S.-China Cyber Agreement

By 2014, the Obama administration had grown extremely frustrated with Chinese cyber intrusions and took a number of actions intended to force Beijing to address U.S. concerns. In May of that year, the Justice Department indicted five PLA officers for cyber hacking. In response, China suspended its participation in the U.S.-China Cyber Working Group. Yet the indictment had an impact on Chinese leaders. Jim Lewis has argued that its effect was "profound" and "exceptionally painful for the Chinese." He suggests that the PLA "felt like it'd been outed. It lost prestige both with other agencies in China and internationally." [193]

In 2015, U.S. leaders substantially increased the pressure. President Obama spoke frequently on the subject and warned of "measures that will indicate to the Chinese that this is not just a matter of us being mildly upset, but is something that will put significant strains on the bilateral relationship if not resolved."[194] These measures reportedly included trade sanctions, which caused substantial concern in Beijing. To signal U.S. willingness to use enhanced measures to stop hacking, President Obama signed an executive order on malicious cyber-enabled activity in April 2015. As he noted when announcing the executive order, "We're giving notice to those who pose significant threats to our security or economy by damaging our critical infrastructure, disrupting or hijacking our computer networks, or stealing the trade secrets of American companies or the personal information of American citizens for profit."[195]

"The Trump administration has made competition with China a central element of its National Security Strategy and National Defense Strategy. Before putting forward specific recommendations on ways to implement Washington's stated goals, however, it is necessary to review recent efforts to alter Chinese behavior."

Speaking at the National Security Agency in early September 2015, the president referenced Chinese cyber espionage and noted, "We can choose to make this an area of competition—which I guarantee you we'll win if we have to—or, alternatively, we can come to an agreement in which we say, this isn't helping

192. The White House, "National Security Strategy of the United States of America," December 2017. (https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf)
193. Benjamin Wittes, "James Lewis on the China Cyber Deal," *Lawfare*, October 5, 2015. (https://www.lawfareblog.com/james-lewis-china-cyber-deal)
194. The White House, Press Release, "Remarks to the Business Roundtable," September 16, 2015. (http://www.presidency.ucsb.edu/ws/index.php?pid=110816)
195. "Red Line Drawn: China Recalculates its Use of Cyber Espionage," *FireEye*, June 2016, page 11. (https://www.fireeye.com/blog/threat-research/2016/06/red-line-drawn-china-espionage.html)

anybody; let's instead try to have some basic rules of the road in terms of how we operate."[196]

Under growing pressure, Meng Jianzhu, the head of the CCP's Political and Legal Affairs Commission, visited Washington to negotiate a deal on cyber security. Days later, Obama and Xi met at the White House and approved what became known as the U.S.-China cyber agreement. In announcing the arrangement, Obama stated unequivocally, "We've agreed that neither the U.S. or the Chinese government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information for commercial advantage."[197] For his part, Xi said that neither the U.S. nor China would "be engaged in or knowingly support online theft of intellectual properties. And we will explore the formulation of appropriate state, behavior and norms of the cyberspace."[198]

These broad statements prompted some concern that the two sides had not settled on a detailed agreement. Nevertheless, in the months that followed, cyber security firms detected fewer cyber intrusions from China. According to one source, the frequency of active network compromises by a group of 72 suspected China-based groups fell from roughly 65 per month in 2013 to under 10 per month in 2016.[199] The co-founder of cyber-security firm CrowdStrike, Dmitri Alperovitch, has called China's behavior change since 2015, "the biggest success we've had in this arena in 30 years," attributing Beijing's new attitude to "the threat of sanctions and the impact on their economy."[200]

"U.S. government officials and other experts conclude that Chinese government hacking against U.S. economic targets continues."

Nevertheless, U.S. government officials and other experts conclude that Chinese government hacking against U.S. economic targets continues.[201] There is evidence that Chinese intrusions remain well below pre-agreement levels, but it is not clear from open-source reporting if China has reduced the number of intrusions or if it is simply more difficult to detect intrusions because Chinese tradecraft has improved. The U.S. intelligence community, for example, has noted that "Private-sector security experts continue to identify ongoing cyber activity from China, although at volumes significantly lower than before the bilateral Chinese-U.S. cyber commitments of September 2015."[202] A report by FireEye in mid-2016 found attacks had become "more focused, calculated, and still successful in compromising corporate networks."[203]

196. David Jackson, "Obama, China's Xi to hold tense meetings on cybersecurity, military," *USA Today*, September 21, 2015. (https://www.usatoday.com/story/news/2015/09/21/obama-china-xi-jinping-white-house-meeting-cybersecurity/72519380/)
197. The White House, Press Release, "Remarks by President Obama and President Xi of the People's Republic of China in Joint Press Conference," September 25, 2015. (https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/remarks-president-obama-and-president-xi-peoples-republic-china-joint)
198. Ibid.
199. Red Line Drawn: China Recalculates its Use of Cyber Espionage," *FireEye*, June 2016, page 9. (https://www.fireeye.com/blog/threat-research/2016/06/red-line-drawn-china-espionage.html)
200. Ken Dilanian, "Russia May Be Hacking Us More, but China Is Hacking Us Much Less," *NBC News*, October 12, 2016. (https://www.nbcnews.com/storyline/hacking-in-america/russia-may-be-hacking-us-more-china-hacking-us-much-n664836)
201. U.S.-Chinese Economic and Security Review Commission, "2016 Annual Report to Congress," November 2016, page 57. (https://www.uscc.gov/sites/default/files/annual_reports/2016%20Annual%20Report%20to%20Congress.pdf); Dmitri Alperovich, "The Latest on Chinese-Affiliated Intrusions into Commercial Companies," *CrowdStrike*, October 19, 2015. (https://www.crowdstrike.com/blog/the-latest-on-chinese-affiliated-intrusions-into-commercial-companies/); "Red Line Drawn: China Recalculates its Use of Cyber Espionage," *FireEye*, June 2016. (https://www.fireeye.com/blog/threat-research/2016/06/red-line-drawn-china-espionage.html)
202. Daniel R. Coast, "Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community," *Statement before Senate Select Committee on Intelligence*, May 11, 2017, page 1. (https://www.dni.gov/files/documents/Newsroom/Testimonies/SSCI%20Unclassified%20SFR%20-%20Final.pdf)
203. "Red Line Drawn: China Recalculates its Use of Cyber Espionage," *FireEye*, June 2016, pages 4, 15. (https://www.fireeye.com/blog/threat-research/2016/06/red-line-drawn-china-espionage.html)

Cyber policy expert Jim Lewis suggests that "Chinese companies used to be able to direct the PLA or MSS to hack into Western competitors," which is no longer the case, but "companies can still put in a request for a target to be hacked but no longer can assign tasks to the teams directly."[204] Another study concludes that China has moved from "vacuum cleaner" espionage to "more precisely targeted intrusion and theft."[205] Rob Knake and Adam Segal write, "China is in fact responsive to U.S. pressure … Chinese actors are more selective and more stealthy at a minimum."[206]

In general, China's "cyber espionage against U.S. companies persists and continues to evolve," and "state-sponsored cyber operators continue to support Beijing's strategic development goals, including its S&T advancement, military modernization, and economic development," a 2018 U.S. Trade Representative report concludes.[207] For example, the Cloud Hopper exploitations (also known as APT10) appear to be Chinese-directed and align with China's current five-year plan.[208] In November 2017, the U.S. Department of Justice unsealed an indictment against three individuals from Chinese internet security firm Boyusec for cyber attacks against financial, engineering, and technology companies.[209] The Justice Department attempted to gain Chinese cooperation in its investigation, but "received no meaningful response," according to a department spokesperson.[210] Jack Goldsmith and Robert Williams note that this indictment "suggests that China is either violating the 2015 deal or exploiting its ambiguities."[211]

Steps to Deter and Defend Against China's Malicious Cyber Activities

Numerous studies have suggested steps to guard against Chinese intellectual property theft and cyber intrusions, but most of the recommendations have not yet been implemented. In 2013, for example, the Commission on the Theft of American Intellectual Property made 21 recommendations, but only eight showed signs of implementation by 2017.[212]

204. William Wilkes, "Hit by Chinese Hackers Seeking Industrial Secrets, German Manufacturers Play Defense," *Fox Business*, September 23, 2017. (https://www.foxbusiness.com/features/hit-by-chinese-hackers-seeking-industrial-secrets-german-manufacturers-play-defense)
205. Mara Hvistendahl, "The Decline in Chinese Cyberattacks: The Story Behind the Numbers," *MIT Technology Review*, October 25, 2016. (https://www.technologyreview.com/s/602705/the-decline-in-chinese-cyberattacks-the-story-behind-the-numbers/)
206. Rob Knake and Adam Segal, "How the Next U.S. President Can Contain China in Cyberspace," *Columbia Journal of International Affairs*, January 29, 2017. (https://jia.sipa.columbia.edu/how-next-us-president-can-contain-china-cyberspace)
207. Office of the United States Trade Representative, "Findings of the Investigation into China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation Under Section 301 of the Trade Act of 1974," March 22, 2018, page 168. (https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF)
208. Kevin Townsend, "Operation Cloud Hopper: China-based Hackers Target Managed Service Providers," *Security Week*, April 6, 2017. (https://www.securityweek.com/operation-cloud-hopper-china-based-hackers-target-managed-service-providers)
209. U.S. Department of Justice, Press Release, "U.S. Charges Three Chinese Hackers Who Work at Internet Security Firm for Hacking Three Corporations for Commercial Advantage," November 27, 2017. (https://www.justice.gov/opa/pr/us-charges-three-chinese-hackers-who-work-internet-security-firm-hacking-three-corporations)
210. Chris Bing, "DOJ reveals indictment against Chinese cyber spies that stole U.S. business secrets," *CyberScoop*, November 27, 2017. (https://www.cyberscoop.com/boyusec-china-doj-indictment/)
211. Jack Goldsmith and Robert D. Williams, "The Chinese Hacking Indictments and the Frail 'Norm' Against Commercial Espionage," *Lawfare*, November 30, 2017. (https://www.lawfareblog.com/chinese-hacking-indictments-and-frail-norm-against-commercial-espionage)
212. Dennis C. Blair and Jon M. Huntsman, Jr., "The Theft of American Intellectual Property: Reassessments of the Challenge and United States Policy," Update to the IP Commission Report, *National Bureau of Asian Research*, February 27, 2017. (http://www.ipcommission.org/report/IP_Commission_Report_Update_2017.pdf)

Previous Recommendations to Address China's Cyber-Enabled Economic Activities[213]

Organizational Fixes

- Designate the national security advisor to coordinate intellectual property protection
- Assign the secretary of commerce responsibility for protecting intellectual property
- Assign the Court of Appeals for the Federal Circuit as the Economic Espionage Act appellate court

Enforcement Measures

- Sequester goods containing stolen intellectual property
- Curtail U.S. banking access for repeat violators
- Enforce strict supply chain accountability for the U.S. government
- Prosecute more trade secret cases
- Apply FTC sanctions to intellectual property theft
- Incentivize improved detection techniques for counterfeit goods
- Penalize intruders into propriety networks, even those not causing damage

Legislative Proposals

- Amend the Economic Espionage Act to provide a private cause of action to allow private groups to take legal action against those causing harm via cyber intrusions
- Expand access to green cards for science, technology, engineering, and math students to keep promising students in the United States after graduation
- Broaden Committee on Foreign Investment in the United State (CFIUS) oversight and consider intellectual property protections in the process
- Support retrieval of stolen intellectual property
- Increase U.S. government resources available for counterintelligence efforts
- Private Actions
- Consider mandatory disclosure of foreign investment or stolen intellectual property
- Implement improved corporate vulnerability-mitigation measures
- Increase protections against transfer of critical technology from universities
- Encourage firms to utilize the private cause of action against Chinese cyber-enabled economic intrusions

Bilateral Negotiations

- Demonstrate willingness to modulate U.S.-China ties if conditions do not improve
- Use senior-level engagement to push China to adopt a more careful patent system
- Prioritize intellectual property theft as a diplomatic priority
- International Engagement
- Work to improve foreign intellectual property theft laws and practices
- Develop regional centers of excellence for intellectual property protection
- Establish a rating system for intellectual property protection by country
- Hold regular meetings of key countries to counter cyber-enabled economic espionage

213. Recommendations drawn from various sources, but primarily from: Dennis C. Blair and Jon M. Huntsman, Jr., "The Theft of American Intellectual Property: Reassessments of the Challenge and United States Policy," Update to the IP Commission Report, *National Bureau of Asian Research*, February 27, 2017. (http://www.ipcommission.org/report/IP_Commission_Report_Update_2017.pdf)

Recent efforts by the U.S. Congress and the executive branch have put in place several recommendations noted above, especially those related to reviewing foreign investment for national security risks. The Foreign Investment Risk Review Modernization Act, for example, which was attached to the FY2019 National Defense Authorization Act, will make the U.S. government's approach to foreign investment more careful and systematic. The Trump administration has praised the legislation, with President Trump noting, "such legislation will provide additional tools to combat the predatory investment practices that threaten our critical technology leadership, national security, and future economic prosperity."[214] The Commerce Department is also reviewing export controls processes in light of recent incidents of industrial espionage and technology leakage. Nevertheless, much work remains.

Unless U.S. leaders prioritize Chinese cyber-enabled economic espionage and coercion, Beijing is unlikely to curb these activities. As a first step, the U.S. government must work to publicize Chinese activities, incentivize private companies to make attacks public so that there can be accurate assessments of the damage, and explain how each piece fits into a larger whole. Currently, the lack of open-source information on the full extent of cyber incidents makes it difficult to conduct comprehensive quantitative analyses. Better data provided directly by victims as well as through public reporting would provide decision makers with a fuller understanding of the threat landscape and enable them to develop policies to deter and defend against cyber intrusions. Specifics on the damage done to individual companies would also help draw additional attention to the issue.

Public-private partnerships provide many opportunities for strengthening protections in both government and the private sector. For example, the Defense Industrial Base Cyber Security Program allows private sector contractors to report to the Department of Defense when they suffer cyber attacks. This information is shared with other defense contractors, allowing them to continually update their systems and protect against intellectual property theft. While this system is limited, it could be expanded to other key industries that may be the target of cyber intrusions. The U.S. government should also work more closely with private companies to help them detect suspicious activity, including through advice on personnel hiring and background screening. Companies should know how to report suspicious activity to law enforcement to more quickly identify suspicious individuals that may be facilitating intellectual property theft.

The U.S. government should also maintain a list of Chinese companies that steal U.S. intellectual property or have used stolen intellectual property.[215] Putting public pressure on these companies for industrial espionage would make them pay for continuing malicious behavior. It would also build awareness and encourage greater debate in the public and expert community, as well as warn the private sector of the risks posed by specific entities. Collectively, these steps would help build consensus about the nature and severity of the threat.

Chinese leaders must also recognize that they will pay a price if malicious behavior continues. Chinese activity across a range of domains operates in the "gray zone" below the threshold that would warrant a major and sustained response.[216] China uses asymmetries, ambiguity, and incrementalism to advance its strategic and economic aims without triggering a conflict with the United States or its friends. The Trump administration's

214. David Lawder and Doina Chiacu, "Trump to use U.S. security review panel to curb China tech investments," *Reuters*, June 27, 2018. (https://www.reuters.com/article/us-usa-trade-china/trump-to-use-u-s-security-review-panel-to-curb-china-tech-investments-idUSKBN1JN1K0)

215. David Beleson and Riley Walters, "This Chinese Company's Intellectual Property Theft is No Isolated Incident," *The Daily Signal*, February 9, 2018. (https://www.dailysignal.com/2018/02/09/chinese-companys-intellectual-property-theft-no-isolated-incident/)

216. Michael Green, Kathleen Hicks, Zack Cooper, John Schaus, and Jake Douglas, "Countering Coercion in Maritime Asia: The Theory and Practice of Gray Zone Deterrence," *Center for Strategic and International Studies*, May 2017. (https://csis-prod.s3.amazonaws.com/s3fs-public/publication/170505_GreenM_CounteringCoercionAsia_Web.pdf?OnoJXfWb4A5gw_n6G.8azgEd8zRIM4wq)

March 2018 U.S. Trade Representative report on China's technology trade practices helped illuminate these issues, but this has often been overshadowed by discussions of other U.S.-China trade issues, such as the bilateral trade deficit.[217] Washington must clearly and consistently demonstrate to Chinese officials that bad behavior in cyber space will damage other elements of the U.S.-China relationship.

The U.S. government has stated that China's malicious cyber activity is undermining both U.S. security and prosperity, so addressing this behavior should be a priority. Although it is unrealistic to expect Beijing to modify activities it believes are central to the CCP's survival, lessons from 2015 demonstrate that Beijing will alter certain behaviors if enough pressure is brought to bear.[218] U.S. leaders should more directly call out Chinese behavior in public statements and joint press conferences, forcing Chinese leaders to either address the behavior or be prepared to answer public questions about it. Washington should also consider deferring some senior-level dialogues on issues important to Chinese leaders until Beijing responds to U.S. concerns. As the executive branch considers further indictments against PLA officers and other malicious cyber actors, Congress should also consider conditioning certain economic interactions with China on its behavior regarding economic espionage and intellectual property theft.

The Trump administration would also be wise to expand its use of multilateral efforts to address Chinese behavior. U.S. leaders should utilize the World Trade Organization to prompt China to account for its practices, much as it is doing with China's discriminating technology licensing practices.[219] U.S. leaders should also seek support from friendly countries in bringing World Trade Organization cases, since this can help to demonstrate that China is violating widely supported rules and norms. At the moment, such cooperation is hampered by U.S. imposition of tariffs on U.S. allies and partners for supposed national security reasons. The challenge presented by Chinese economic statecraft far outweighs these disagreements.

Conclusion

Washington is starting to take a tougher public line against Beijing. The National Security Strategy, for example, insists that the United States "will no longer turn a blind eye to violations, cheating, or economic aggression."[220] Unfortunately, the Trump administration continues to focus on the bilateral trade deficit, sometimes to the detriment of the underlying Chinese economic strategy that created this trade imbalance. Beijing is likely to offer Washington a deal that will decrease the trade deficit but not address the longer-term structural problems in the U.S.-China economic relationship. If the Trump administration accepts such a deal, the United States and its allies may lose badly needed leverage.[221] It is critical that the Trump administration and the U.S. Congress work together to demonstrate to China that the status quo cannot continue. Given the dramatic national security implications of Chinese cyber intrusions against U.S. economic assets, it is time the United States treated this as a true priority.

217. For the Trump administration's most-concerted effort to win public support for addressing U.S.-China trade imbalances, see: The White House, "Fact Sheet: President Donald J. Trump is Standing Up for American Innovation," March 22, 2018. (https://www.whitehouse.gov/briefings-statements/president-donald-j-trump-standing-american-innovation/)

218. One of the challenges U.S. policymakers will face is not only convincing China to curb its own malicious cyber activities but also to cease its enabling of North Korean hacking. The way that China supports or turns a blind eye toward Pyongyang's cyber attacks is beyond the scope of this paper but will be addressed in a forthcoming monograph by other scholars with FDD's cyber-enabled economic warfare project.

219. Vicki Needham, "US launches trade case against China over licensing practices," *The Hill*, March 23, 2018. (http://thehill.com/policy/finance/380009-us-launches-trade-case-against-china-over-licensing-practices)

220. The White House, "National Security Strategy of the United States of America," December 2017, page 17. (https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf)

221. Derek Scissors, "The Trump administration fails on China," *American Enterprise Institute*, May 22, 2018. (http://www.aei.org/publication/trump-administration-fails-on-china/)

Acknowledgments

This study is the result of several years of collaboration with a variety of experts who deserve acknowledgement. The author is particularly thankful to Samantha Ravich and Annie Fixler for supporting the project and providing advice throughout. In addition, many others at the Foundation for Defense of Democracies assisted by reviewing drafts, providing research, or preparing the final product, including Joathan Schanzer, David Adesnik, Nicole Salter, Daniel Ackerman, and Erin Blumenthal. The author is also thankful to external reviewers Juan C. Zarate, Larry Wortzel, John Carlin, Jake Bebber, and Carolyn Leddy for their detailed advice and guidance, as well as to Samm Sacks, Eric Lorber, Michael Sulmeyer, Bonnie Glaser, and others who provided more general insights into issues covered in the study. An early version of this research was shared at a conference held jointly by the Hoover Institution and Lawfare, which provided a valuable sounding board for some of the initial concepts. Finally, there are a variety of others in the U.S. government, particularly in the White House, Defense Department, State Department, Department of the Treasury, Department of Justice, and the intelligence community who are deserving of thanks – as well as a number of experts in foreign governments and research institutions – but who will here remain nameless. Where errors remain despite these interventions, those errors remain my own.

This report is part of a series of studies on adversarial strategies from FDD's project on cyber-enabled economic warfare. The project aims to promote a greater understanding within the U.S. government, private sector, and allied countries of the threats and opportunities that the new environment poses and assist as policymakers develop and implement a winning strategy for the United States within this domain.

Cover Illustration by Daniel Ackerman

About The Author

Dr. Zack Cooper is a research fellow at the American Enterprise Institute (AEI). He also serves on the Board of Advisors of the Center on Sanctions and Illicit Finance at the Foundation for Defense of Democracies. Prior to joining AEI, Dr. Cooper worked as a senior fellow for Asian security at the Center for Strategic and International Studies and as a research fellow at the Center for Strategic and Budgetary Assessments. He previously served on the White House staff as an assistant to the deputy national security adviser for combating terrorism. He also worked as a civil servant in the Pentagon, first as a foreign affairs specialist and then as a special assistant to the principal deputy under secretary of defense for policy. He received a BA from Stanford University and an MPA, MA, and PhD from Princeton University.

About the Foundation for Defense of Democracies' Center on Sanctions and Illicit Finance

The Center on Sanctions and Illicit Finance (CSIF) at the Foundation for Defense of Democracies (FDD) works to expand the understanding of economic warfare in the 21st century to develop further the doctrines and strategies of American financial and economic suasion. Launched in 2014, CSIF builds upon FDD's success as a leading policy institute on the use of financial measures in foreign policy. Our mission is to strengthen and preserve the ability of America and its allies to deploy economic tools to promote national security, develop strategies to isolate rogue actors, and identify and guard against economic threats and vulnerabilities.

CSIF's research and analysis catalyzes global action, in both the public and private sectors, to address core challenges to effective implementation of financial and economic power at a time when these ideas are increasingly central to U.S. national security interests. Our experts provide policy and subject matter expertise that highlights the critical intersection between illicit financial activities and national security, including money laundering, terrorist financing, sanctions evasion, proliferation financing, cyber-enabled economic warfare, corruption and kleptocracy. CSIF is also exploring the changing technological landscape to understand its effects on financial transparency and the fundamentals of U.S. economic power.

CSIF is led by Mark Dubowitz, Juan Zarate, Chip Poncy, Jonathan Schanzer and Yaya J. Fanusie, and also relies on regional and sanctions expertise within FDD including a core cadre of financial, economic, and area experts and analysts. It is guided by a senior, expert Board of Advisors, that provides strategic guidance, leads initiatives, and assists in outreach.

For more information, please visit www.defenddemocracy.org

FDD
FOUNDATION FOR
DEFENSE OF DEMOCRACIES

P.O. Box 33249
Washington, DC 20033-3249
(202) 207-0190
www.defenddemocracy.org