COUNCIL on FOREIGN RELATIONS

U.S. Responses to the China Cyber Challenge: Diplomatic Efforts to Establish Norms in Cyberspace

Prepared statement by
Adam Segal
Ira A. Lipman Chair in Emerging Technologies and National Security and Director, Digital and Cyberspace Policy Program
Council on Foreign Relations

Before the
U.S. China Economic Security Review Commission
February 17, 2022

Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States

The United States and China differ on the norms of responsible state behavior in cyberspace. In particular, Washington and Beijing hold conflicting views on the applicability of international law to cyberspace as well as the legitimacy of cyber-enabled industrial espionage. For almost a decade, the United States has unsuccessfully tried to shape Chinese behavior with a combination of diplomatic dialogue and attempts to impose costs more directly. The strategy appeared to succeed briefly in 2015, when President Xi stood next to President Obama and declared that China would not support cyber-enabled espionage, but today Chinese state-backed hackers continue to conduct operations that threaten U.S. economic security. In addition, while the two sides have both agreed to a shared set of norms of state behavior developed through a United Nations process, they remain sharply divided over how to move forward.

U.S. diplomatic efforts will continue to have little impact on Chinese behavior. Moving forward, the United States should look for more effective means to disrupt Chinese operators, impose costs on those who benefit from the theft of U.S. intellectual property, and improve U.S. cyber defenses. In addition, multilateral discussions need to be supplemented with a direct dialogue with Beijing on cyber doctrine and operations.

International Law and Cyber Conflict

The United States' position is that international law is applicable to cyberspace, and Washington believes that states should discuss how they understand their rights and obligations, including in regard to self-defense, use of force, non-interference, and armed conflict. The United States also holds that sovereignty is a principle of international law, and so there is no absolute prohibition on cyber operations that may touch on other's territory as a matter of international law. While violations would depend on circumstances, the United States appears to be referring to instances when "defending forward" activities in another state's territory have no effects or de minimize effects.

China agrees that international law is applicable in cyberspace, but has resisted concrete descriptions of state rights and responsibilities. In fact, Beijing has tended to characterize the call for greater explication of rights and responsibilities, especially jus ad bellum (the body of law that addresses uses of force triggering the use force in self-defense) and jus in bello (the body of law governing the conduct of hostilities), as leading to the "militarization of cyberspace." In an October 2021 prepared statement on China's position, for example, the Ministry of Foreign Affairs warned of the need to "handle the applicability of the law of armed conflicts and jus ad bellum with prudence, and prevent escalation of conflicts or turning cyberspace into a new battlefield."[1] Beijing has also tended to stress that sovereignty is a rule, and so would assert that cyber operations, even if they had limited effects, would be violations of sovereignty.

In addition, along with Moscow, Beijing has often suggested that the unique characteristics of cyberspace require a new international treaty. In September 2011, China and Russia, supported by Tajikistan and Uzbekistan, submitted a letter proposing a Draft International Code of Conduct for Information Security to the United Nations General Assembly.[2] The code supported a UN process in developing norms and rules for information, calling on states to agree that they will not "use information and communications technologies, including networks, to carry out hostile activities or acts of aggression, pose threats to international peace and security or proliferate information weapons or related technologies." The code was submitted to the UN again in 2015 by the Shanghai Cooperation Organization (SCO), the Eurasian regional organization that includes China, Russia, Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan.[3]

Norms and State Behavior

China has been a participant in the UN process to discuss the rules of the road for cyberspace, the Group of Government Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security, since the first meeting in 2004. In June 2013, for the first time, the GGE, which included China, Russia, United States, and representatives from twelve other nations, issued a consensus report. The members of the group agreed that "international law, and in particular, the United Nations Charter applies to cyberspace."[4] After the report was issued, U.S. officials used the consensus to argue that by agreeing to the UN Charters, the signers were also accepting the Geneva Conventions and the applicability of the Laws of Armed Conflict to cyberspace. In contrast, Chinese official highlighted the GGE's embrace of state authority, non-interference, and equality, not the international law implications of accepting the UN Charter's application to cyberspace.[5]

The 2015 GGE group was tasked with examining "norms, rules or principles for responsible [behavior] of States" as well as "how international law applies to the use of information and communications technologies by States." Beijing, along with Moscow, signed off on four norms promoted by Washington in the 2015 report. Those norms included: norms of state responsibility and the duty to assist as well as that states should not intentionally damage or impair others' critical infrastructure or target another

state's computer emergency response teams during peacetime. But China and Russia, along with Pakistan, Malaysia, and Belarus, opposed a US effort to include a reference to Article 51 of the U.N. Charter, which authorizes the use of force in self-defense against an "armed attack."

China and Russia also used the 2015 GGE to express concern about the increasing willingness of the United States to name and shame state-backed hackers. As it has called out Chinese, Iranian, Russia, and North Korean hackers, Washington has argued that attribution is not as difficult as once believed. When Chinese hackers have been publicly name, Chinese officials have often responded that such efforts are "unprofessional" and "unscientific." The 2015 report notes that while states must meet their obligations for internationally wrongful acts attributable to them, "indication that an ICT activity was launched or otherwise originates from the territory or the ICT infrastructure of a State may be insufficient in itself to attribute the activity to that State." Given this challenge, the report concludes that "accusations of organizing and implementing wrongful acts brought against States should be substantiated."[6]

In the run-up to the 2017 GGE meeting, U.S. officials warned that they hoped the group would not identify new norms but rather explain how states should adopt existing rules. State Department Deputy Coordinator for Cyber Issues Michele Markoff said, "We don't need a continual norms machine ramping out a lot of norms. What we need to do is consolidate what we've done and get states to implement."[7] The group, however, failed to issue a consensus report, and divisions over the question of the applicability of the law of countermeasures and the inherent right of self-defense proved especially contentious. The Cuban representative publicly opposed these measures, arguing that they would lead to a militarization of cyberspace that would "legitimize … unilateral punitive force actions."[8] This is a view shared by Russia and China, and they may have supported Cuba making it from behind the scenes.[9]

After the failure of the group to reach a consensus, the norms discussion split into two parallel processes. Russia proposed an Open-Ended Working Group (OEWG) to study the existing norms contained in the previous UN GGE reports, identify new norms, and study the possibility of "establishing regular institutional dialogue ... under the auspices of the United Nations." The United States entered a proposal to continue the work of the GGE, and both resolutions passed.

While many feared that the two processes would result in competing norms, the chairs of the two groups closely coordinated with each other. The OEWG's report reaffirmed the norms of the 2015 GGE report, but it did omit references to international humanitarian law, the laws designed to protect civilians during times of armed conflict. As with the 2017 GGE report, opposition to the incorporation of international humanitarian probably stems from the argument that its inclusion would normalize the militarization of cyberspace and legitimize cyber attacks.

China, along with Russia, will remain unwilling to discuss any further how international law applies in cyberspace, and instead will want to shift conversations to the need for a new treaty covering cyber norms. The joint statement issued by China and Russia during Putin's February 2022 visit, for example, stressed the "principles of the non-use of force, respect for national sovereignty and fundamental human rights and freedoms, and non-interference in the internal affairs of other States, as enshrined in the UN Charter, are applicable to the information space application of UN Charter and state sovereignty over information space." The two sides also called for consolidation of norms into a binding treaty: the two sides "consider it necessary to consolidate the efforts of the international community to develop new norms of responsible behavior of States, including legal ones, as well as a universal international legal instrument regulating the activities of States in the field of ICT."[10]

Bilateral Discussions

Outside of the UN process, Washington has tried to engage Beijing in bilateral discussion on cyber conflict. U.S. officials and analysts have long worried that, without shared understanding of thresholds, signaling, and escalation in cyberspace, a cyber incident could spur a kinetic conflict. Cyber issues were discussed at the Strategic and Economic Dialogue, which met eight times between 2009 and 2016. In addition, the two sides agreed to a cyber expert working group during the September 2015 summit between presidents Xi and Obama, but that group only met once in May 2016, led by the State Department and the Ministry of Foreign Affairs. President Xi and President Trump agreed to four dialogues, including the Law Enforcement and Cyber Strategic Dialogue and the Diplomatic and Security Dialogue. The latter reportedly met in June 2017 and discussed issues of stability and international standards; the former, led by the Department of Justice and the Department of Homeland Security, focused on intellectual property theft and crime.[11]

The pattern of these bilateral talks mirrors many of the challenges that affected military-to-military and strategic dialogues between the United States and China.[12] Bilateral cybersecurity discussions were clearly something Washington wanted more than Beijing. While the United States wanted to engage broadly with the People's Liberation Army (PLA), the talks were generally limited to diplomats through the Strategic and Economic Dialogue. The PLA representatives who attended these talks were from the foreign affairs office, not cyber operations. According to the *New York Times*, in 2014 the Pentagon briefed PLA officials on American doctrine on the use of offensive cyber operations in an effort to convince the Chinese that the United States was exercising restraint in cyberspace. The PLA did not reciprocate.[13] Moreover, China often treated the talks as a bargaining point, something to be offered or withdrawn depending on the state of the relationship. China, for example, cancelled a military dialogue on cyber issues to signal displeasure after the Department Justice indicted five alleged PLA hackers for cyberespionage in May 2014.

Given the difficulties of the official dialogues, there have also been a number of semi-formal channels. Starting in 2009, Center for Strategic and International Studies and China Institutes of Contemporary International Relations held at least nine Track 1.5 and 2 cybersecurity dialogues, attended by think tankers and academics, as well as U.S. and Chinese officials from State, Defense, DHS, FBI, and Ministry of Foreign Affairs, Ministry of Public Security, Cyberspace Administration of China, and PLA respectively.[14] These meetings usually included an update on national and international developments in cybersecurity, as well as broader discussions on issues such as norm, strategic stability and use of force.

The Norms of Cyber Espionage and the Bilateral Agreement

Washington's effort to establish a normative difference between espionage conducted for competitive advantage and espionage for national security purposes is its longest standing, highest profile effort with Beijing. In the United States' framing, cyber espionage for national security purposes is to be expected by all states and is fair game. Hacking private companies for commercial gain, on the other hand, is illegitimate. This leads to the somewhat incongruous scene of U.S. officials essentially tipping their hats to certain types of operations. When China, for example, was suspected of being behind the hack of the Office of Personnel Management, Director of National Intelligence James Clapper stated "you have to kind of salute the Chinese for what they did. If we had the opportunity to do that, I don't think we'd hesitate for a minute."[15]

In the face of a massive, multi-year cyber campaign conducted to steal U.S. intellectual property and business secrets—a campaign former director of the NSA and commander of Cyber Command General Keith Alexander once described as the "greatest transfer of wealth in history"—the United States at first

hesitated to publicly call out or confront China. The hesitation derived from a fear that public attribution would reveal U.S. technical measures as well as an unwillingness to risk other, higher priority issues that required Beijing's cooperation, such as restarting the economy after the global recession and containing Iran's and North Korea's nuclear programs.

That calculus changed around 2013. In February, cybersecurity firm Mandiant released a report stating that Unit 61398 of the PLA was behind attacks on 115 companies in the United States, and around the same time, the Department of Homeland Security provided internet service providers with the internet addresses of hacking groups in China In a speech at the Asia Society in March, National Security Advisor Thomas Donilon warned of "cyber intrusions emanating from China on an unprecedented scale" risked destabilizing the bilateral relationship.[16] Months later, U.S. President Barack Obama confronted Chinese President Xi Jinping with the issue at the Sunnylands Summit. Then, in May 2014, in a significant escalation of public pressure, the Department of Justice indicted five People's Liberation Army officers for stealing trade secrets from Westinghouse, U.S. Steel, and other companies.[17]

In the summer of 2015, news reports suggested that the administration was ready to use Executive Order 13694, which authorizes sanctions against companies or individuals that profit from cyber theft, to sanction state-owned enterprises and senior Chinese officials associated with cyber theft.[18] These punishments would have overshadowed President Xi's first summit in Washington, and in response, Beijing dispatched Meng Jianzhu, one of the Chinese Communist Party's highest-ranking officials, to negotiate an agreement. In the agreement, which was announced by both presidents in the Rose Garden, China and the United States announced that neither would "conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors."[19] In the months after the summit, China reached similar agreements with Australia, Canada, and the United Kingdom. Beijing also signed off on Group of Seven and Group of Twenty statements that proscribed cyber industrial espionage.[20]

Despite initial skepticism about the agreement's efficacy, cybersecurity companies recorded a steep decline in Chinese attacks against U.S. companies in the first year after it was concluded. FireEye released a report in June 2016 that showed that the number of network compromises by the China-based hacking groups they tracked dropped from sixty in February 2013 to less than ten by May 2016.[21] However, experts warned that the decrease in the number of publicly disclosed attacks might be the result of Chinese attackers becoming more stealth. The decline also appeared to predate the agreement, suggesting that internal forces, such as the consolidation of control over PLA cyber units through the creation of the Strategic Support Force (the PLA's space, cyber, and electronic warfare arm), was as much as a rationale as U.S. diplomatic pressure.

The norm against cyber economic espionage is not universally held. A number of close U.S. allies and partners engage in the practice. Moreover, Chinese officials never seem to have embraced the distinction, often calling the United States' denunciations of Chinese cyber operations as violating international norms as hypocritical, especially in the wake of the revelations of widespread U.S. espionage activities by Edward Snowden. By 2018, it was clear that Chinese cyber espionage had returned, with Chinese groups targeting companies operating in sectors that Beijing believes are important for future economic competitiveness, such as aerospace, semiconductors, and information technology.

The hiatus in Chinese cyber operations may have had two sources.[22] First, Beijing might never have intended to give up cyber espionage entirely but instead saw an opportunity to gain diplomatic advantage in implementing changes it already planned to make, shifting espionage from PLA hackers to

more skilled operators in the Ministry of State Security (MSS). Although this would result in a temporary downturn in activity as hacking infrastructure was reoriented, its main purpose was to allow the PLA to focus on warfighting operations and reduce the number of incidents the United States could attribute to China. The agreement also prevented Xi's visit from being ruined or cancelled. In effect, Beijing always intended to continue commercial espionage—it just intended to stop getting caught.

Second, the return to industrial hacking might have been a reaction to the increased political and trade tensions between Washington and Beijing. With the Trump administration restricting Chinese investment in high-technology sectors, blocking Chinese telecommunication companies from doing business in the United States, levying tariffs against Chinese exporters, and blocking the sale of sensitive technology to Chinese firms, Chinese policymakers might have believed they had little to gain from continuing to honor the agreement.

Indictments and Joint Attribution

U.S. discussions with and pressure on China have been accompanied by public attribution and indictments of Chinese hackers. These include the indictment in 2014 of five PLA hackers for economic espionage; in November 2017 of three Chinese hackers who worked at the cybersecurity firm Boyusec for the theft of confidential business information; in December 2018 of two Chinese individuals for theft of intellectual property; in May 2019 for the hack on Anthem; in February 2020 of four military hackers for targeting Equifax; in July 2020 of two MSS hackers for targeting intellectual property, including COVID-19 research; in September 2020 of members of a Chinese hacking group known as APT 41; and in July 2021 of hackers associated with Hainan MSS.

The December 2018 indictment was part of the United States' effort to include friends and allies in public attribution of cyber-espionage operations. The campaign, known as Cloud Hopper, was a supply chain attack that targeted managed service providers like Hewlett Packard and IBM that provide cloud and other IT services to customers. The DOJ indicted two Chinese individuals, Zhu Hua and Zhang Shilong. According to the indictment, Zhu and Zhang were members of a hacking group operating in China known as Advanced Persistent Threat 10 (APT10). The defendants worked for Huaying Haitai Science and Technology Development Company and acted in association with the Ministry of State Security's Tianjin State Security Bureau.[23] Thirteen additional countries either joined the attribution or expressed concern about malicious cyber behavior. The five eyes joined in the attribution; Berlin and Tokyo issued statements approving of and supporting the attribution.

The European Union also participated, although slowly, and at first, indirectly. Almost five months after the U.S. attribution, in April 2019, Federica Mogherini, High Representative of the Union for Foreign Affairs and Security Policy, expressed concern about "the rise in malicious behavior in cyberspace that aim at undermining the EU's integrity, security and economic competitiveness, including increasing acts of cyber-enabled theft of intellectual property."[24] The statement did not name China. In November 2020, almost two years after the initial US attribution, the EU imposed travel restrictions on Zhang, and another individual, Gao Qiang, who it claimed was active in Cloud Hopper and was associated with APT 10 and Hauying Haitai.[25]

In July 2021, the United States attributed "with a high degree of confidence" the Microsoft Exchange Server attack to the MSS. The attack exploited a zero day vulnerability and appears initially to have targeted think tanks and other espionage targets. Moreover, knowing that Microsoft was pushing out a patch for the vulnerability, the Chinese scanned almost the entire internet to find exposed servers to be compromised. The White House called out China's "irresponsible behavior in cyber space" as being

"inconsistent with its stated objective of being seen as a responsible leader in the world."[26] The statement also accused Beijing of using criminal groups as hacking proxies, and announced an indictment of four MSS hackers for a multi-year espionage campaign that spanned 2011 to 2018, separate from Microsoft Exchange hack. The Biden administration has not yet officially responded to the hacks, perhaps because it does appear to be an act of political espionage, not an attempt to steal intellectual property.

The White House also trumpeted that an "unprecedented" group of allies and partners joined the attribution of the Microsoft Exchange Server attack. The group included Canada, UK, EU, and, for the first time, NATO. Yet there was some difference on how directly partners were willing to assign responsibility to Chinese actors. NATO did not directly attribute to China, but rather acknowledged national statements by allies "attributing responsibility for the Microsoft Exchange Server compromise to the People's Republic of China."[27] The EU assessed that the activity had been "conducted from the territory of China for the purpose of intellectual property theft and espionage," rather than directly calling out the Ministry of State Security.[28]

The indictments and public attribution have not deterred or slowed Chinese operations. Proponents of the strategy argue, however, that the release of evidence in support of the indictments is a useful demonstration of U.S. attribution capabilities. They also may convince others to join attribution based on intelligence shared by the U.S. The goal eventually is to build a broader set of partners who are both prepared to call out malicious actions and act to punish China.

Persistent Engagement and Chinese Behavior

In 2018, the Pentagon adopted a cyber strategy that was more offense oriented. Describing a competitive environment in which Cyber Command would persistently engage with adversaries, the strategy states that U.S. operators "will disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict." Most of the public information on how persistent engagement has been implemented has concerned disrupting Russian influence operations, but former National Security Advisor John Bolton suggested that Cyber Command was also launching operations against Chinese hackers.

Persistent engagement has two expected paths to change Chinese behavior. First, and most directly, defending forward and disrupting operations should impost costs on Chinese hackers. As Chinese hacking groups find it harder to operate, the total number of attacks should go down. Second, over time, persistent engagement is expected to create shared understandings of acceptable cyber behavior. Tit-for-tat, action-reaction cycles will eventually make clear to both sides what the other sees as legitimate actions in cyberspace.

What is Next?

Moving forward, it is clear that the United States shares with its friends and allies a similar perception of the Chinese threat in cyberspace. The 2021 report from the National Cyber Security Centre, for example, states that "China remained a highly sophisticated actor in cyberspace with increasing ambition to project its influence beyond its borders and a proven interest in the UK's commercial secrets. How China evolves in the next decade will probably be the single biggest driver of the UK's future cyber security." In addition, for the first time, the 2021 Brussels Communique framed Chinese actions as a challenge to NATO's security interests, with the alliance calling out "cyber, hybrid, and other asymmetric threats, including disinformation campaigns, and by the malicious use of ever-more sophisticated emerging and disruptive technologies."[29]

While U.S. friends and allies will be more willing to call out Chinese industrial espionage, they are likely to remain hesitant to sanction Beijing on cyber issues. The coordination of attribution among states with different methods and procedures is difficult, though in the wake of the SolarWinds hack, the White House announced that it was providing training on the policy and technical aspects of publicly attributing cyber incidents.[30] Moreover, high economic interdependence with China, fear of retaliation, and a desire to make progress on higher priority issues all combine to make it difficult for countries to follow through with sanctions.

The United States should not expect Beijing to accept the norm against cyber-enabled industrial espionage. Joint attribution and indictments do little to impose costs on Chinese hackers, though they help in binding allies and partners together in shared norms and in preparing the ground eventually for collective action. To deal with cyber-enabled industrial espionage, the United States should rely on persistent engagement and disruption, the imposition of costs on those who benefit from the theft, and improved defense. The administration should authorize the Treasury Department to sanction companies, universities, researchers, and individuals who benefit from cyberattacks designed to steal U.S. intellectual property. The Department of Commerce could also bar the exports of U.S. technology to companies that benefit from cyber espionage.

The U.S. government should help small companies increase their cyber defenses against Chinese hackers and strengthen counterintelligence to identify sectors and companies under threat. Small companies and start-ups in AI, quantum, semiconductor, telecommunications, and other sectors central to Chinese technology strategies are unlikely to be aware of the threat of Chinese actors or have the resources and expertise to reduce vulnerabilities.[31]

Washington should be similarly clear eyed about the multilateral norms process and international security. In the near term, Beijing is unlikely to drop its long held position that cyberspace requires a new treaty or abandon its resistance to explicating the application of international law to cyberspace. As with joint attribution, the GGE and OEWG processes are more successful in defining acceptable behavior among allies and partners than constraining malicious actions by potential adversaries.

The United States should continue to engage China through the UN process, but the priority should be direct dialogues that bring cyber operators together.[32] These dialogues should be designed to improve mutual understanding of each other's cyber operations and doctrine, and may involve confidence-building measures such as greater information exchanges during cyber incidents and identifying points of contact for communication during a cyber crisis.

[1] Available at National position of the People's Republic of China (2021), https://cyberlaw.ccdcoe.org/wiki/National_position_of_the_People%27s_Republic_of_China_(2021)
[2] https://www.rusemb.org.uk/policycontact/49%20

[3]U.N. General Assembly, "Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General," U.N. Doc. A/69/273 (2015), http://www.un.org/Docs/journal/asp/ws.asp?m=A/69/723.
[4] https://undocs.org/A/68/98
[5] Adam Segal, *Chinese Cyber Diplomacy In A New Era Of Uncertainty*, Hoover Institution, June 2, 2017, https://www.hoover.org/research/chinese-cyber-diplomacy-new-era-uncertainty
[6] https://undocs.org/A/70/174
[7] Joseph Marks, "The US Does An About-Face on New Cyber Norms," *DefenseOne*, February 7, 2017, https://www.defenseone.com/technology/2017/02/us-does-about-face-new-cyber-norms/135227/
[8] https://www.justsecurity.org/wp-content/uploads/2017/06/Cuban-Expert-Declaration.pdf
[9] Elaine Korak," UN GGE on Cybersecurity: The End of an Era?" *The Diplomat*
[10] Joint Statement of the Russian Federation and the People's Republic of China on the International Relations Entering a New Era and the Global Sustainable Development, February 4, 2022, http://en.kremlin.ru/supplement/5770?s=08
[11] Secretary of State Rex Tillerson and Secretary of Defense Jim Mattis at a Joint Press Availability (U.S. State Department, June 21, 2017) (www.state.gov/secretary/remarks/2017/06/272103.htm); "First U.S.-China Law Enforcement and Cybersecurity Dialogue: Summary of Outcomes, Department of Justice," October 6, 2018. (www.justice.gov/opa/pr/first-us-china-law-enforcement-and-cybersecurity-dialogue).
[12] Kurt Campbell and Richard Weitz, "The Limits of U.S.-China Military Cooperation: Lessons from 1995–1999," *Washington Quarterly*, Winter 2005-2006.
[13] David E. Sanger, "U.S. Tries Candor to Assure China on Cyberattacks," *New York Times*, April 6, 2014, https://www.nytimes.com/2014/04/07/world/us-tries-candor-to-assure-china-on-cyberattacks.html?_r=0.
[14] https://www.csis.org/programs/strategic-technologies-program/cybersecurity-and-governance/other-projects-cybersecurity-3
[15] Julianne Pepitone, "China is 'Leading Suspect in OPM Hacks, Says Intelligence Chief James Clapper," *NBC News*, June 25, 2015, https://www.nbcnews.com/tech/security/clapper-china-leading-suspect-opm-hack-n381881
[16] "The United States and Asia-Pacific in 2013," Complete Transcript: Thomas Donilon at Asia Society New York, March 11, 2013, https://asiasociety.org/new-york/complete-transcript-thomas-donilon-asia-society-new-york
[17] Mark Clayton, "US indicts five in China's secret 'Unit 61398' for cyber-spying on US firms," *Christian Science Monitor*, May 19, 2014, https://www.csmonitor.com/World/Passcode/2014/0519/US-indicts-five-in-China-s-secret-Unit-61398-for-cyber-spying-on-US-firms
[18]White House, Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities, April 1, 2015, https://home.treasury.gov/system/files/126/cyber_eo.pdf
[19] https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states
[20] Cody Poplin, "Cyber Sections of the Latest G20 Leaders' Communiqué," *Lawfare*, November 17, 2015, https://www.lawfareblog.com/cyber-sections-latest-g20-leaders-communiqu%C3%A9
[21] Mandiant, *Red Line Drawn: China recalculates its use of cyber espionage*, https://www.mandiant.com/resources/red-line-drawn-china-recalculates-its-use-of-cyber-espionage
[22] Next two paragraphs come from Lorand Laskai and Adam Segal, "A New Old Threat: Countering the Return of Chinese Cyber Industrial Espionage," Council on Foreign Relations, December 6, 2018, https://www.cfr.org/report/threat-chinese-espionage
[23]Department of Justice, Two Chinese Hackers Associated With the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information, December 20, 2018, https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion
[24] Council of the European Union, "Declaration by the High Representative on behalf of the EU on respect for the rules-based order in cyberspace", press release, Brussels, 12 April 2019, https://www.consilium.europa.eu/en/press/press-releases/2019/04/12/declaration-by-the-high-representative-on-behalf-of-the-eu-on-respect-for-the-rules-based-order-in-cyberspace/
[25] Council of the European Union, "Council Implement-ing Regulation (EU) 2020/1744 of 20 November 2020 Imple-menting Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States", Official Journal of the European Union, no. L 393/1 (23 November 2020), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L%5F.2020.393.01.0001. 01.ENG&toc=OJ%3AL%3A2020%3A393%3ATOC
[26] The White House, The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China, July 19, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/19/the-united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china/
[27] Statement by the North Atlantic Council in solidarity with those affected by recent malicious cyber activities including the Microsoft Exchange Server compromise, July 19, 2021, https://www.nato.int/cps/en/natohq/news_185863.htm
[28] Council of the EU, China: Declaration by the High Representative on behalf of the European Union urging Chinese authorities to take action against malicious cyber activities undertaken from its territory, July 19, 2021,

https://www.consilium.europa.eu/en/press/press-releases/2021/07/19/declaration-by-the-high-representative-on-behalf-of-the-eu-urging-china-to-take-action-against-malicious-cyber-activities-undertaken-from-its-territory/

[29] Bussels Summit Communique, June 14, 2021, https://www.nato.int/cps/en/natohq/news_185000.htm

[30] White House, Fact Sheet: Imposing Costs for Harmful Foreign Activities by the Russian Government, April 15, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/

[31] Laskai and Segal, New Old Threat

[32] Adam Segal, "Strategic Stability in Cyberspace," in *Enhancing U.S.-China Strategic Stability in an Era of Strategic Competition*, United States Institue of Peace, April 26, 2021, https://www.usip.org/sites/default/files/2021-04/pw_172-enhancing_us-china_strategic_stability_in_an_era_of_strategic_competition_us_and_chinese_perspectives.pdf