A HOOVER INSTITUTION ESSAY

The Case for Pragmatism and an Opportunity for Sino-US Leadership

PROTECTING FINANCIAL STABILITY AGAINST CYBER THREATS

TIM MAURER

Aegis Series Paper No. 1808

On March 22, 2018, President Trump directed the US trade representative to impose tariffs on about $50 billion worth of Chinese imports.[1] With China announcing retaliatory action shortly thereafter, observers feared that this was the opening salvo of a global trade war.[2] As the United States and China enter this new period of tension, the time will come when both sides will search for new opportunities for collaboration to mend ties. Looking ahead, one such opportunity is an area of common interest: protecting the financial system against emerging threats. This shared interest could form the basis for a joint initiative between China and the United States bilaterally as well as on the global stage.

Increasingly daring, disruptive, and destructive cyberattacks pose an unprecedented threat to the global financial system. For example, in April 2016, a group of hackers exploited access to the SWIFT network, the nervous system of global finance, in an attempt to steal $1 billion.[3] How disruptive and widespread malware can become was illustrated a year later by the WannaCry malware, which infected systems around the world and caused widespread disruption, including forcing hospitals in the United Kingdom to turn patients away.[4] In both cases, North Korea stood accused as the culprit.

That is why in March 2017, the G20 Finance Ministers and Central Bank Governors warned that "the malicious use of Information and Communication Technologies (ICT) could disrupt financial services crucial to both national and international financial systems, undermine security and confidence and endanger financial stability."[5] This is the first time the G20 Finance Ministers and Central Bank Governors expressed such concern. They did so with the memory of the worst financial crisis in nearly a century, the 2007–2008 global economic crisis, still fresh in their minds. Currently, states still struggle to effectively counter such threats. Existing exercises fail to adequately take into account the international connections and

dependencies of the global financial system's network. Mechanisms to coordinate and cooperate remain nascent.

This challenge presents an opportunity for the United States and China as the world's two largest economies to work together, rallying behind their shared interest in protecting financial stability, and demonstrate global leadership on this important issue.[6] China and the United States are among the only countries represented in the various institutions necessary to accomplish such an endeavor, and they certainly carry the most weight for such an initiative to be effective. Working together on this issue set would benefit both countries by adding a new element of common interest to their bilateral cooperation with the potential to inject more stability into an otherwise competitive and often contentious relationship. Cooperating and focusing on this common interest could help build confidence and trust between the two countries as part of their bilateral relationship generally and in the context of cybersecurity specifically.

The scope and pace of such cooperation will depend on the level of ambition of both countries. The less ambitious goal would be for China and the United States to express their intention to cooperate to protect global financial stability against cyber threats and to add this item to their bilateral dialogue. They could further encourage the other G20 members to discuss this issue within the G20. A more ambitious agenda would be for China and the United States to advance a more robust bilateral agenda as well as a specific proposal for a G20 communiqué condemning cyberattacks that could pose a risk to financial stability and explicitly committing to cooperate when such incidents occur. Manipulating the integrity of financial institution data and targeting the availability of critical systems pose particular risks. Implementing these commitments could either be pursued with the Financial Stability Board acting as a convener or via an ad hoc mechanism such as a temporary task force building on the successful model used for the creation of the Financial Action Task Force.

Ultimately, this is an issue putting each country's interests first and pursuing a shared interest at the international level.[7] Bilateral cooperation between the United States and China on this issue would align with remarks by US administration officials that the new administration will prioritize bilateral over multilateral engagement.[8] Beijing, in its 2017 international strategy for cyberspace, has also explicitly stated as one of its objectives that "countries should work together to ensure cybersecurity through constructive consultation and cooperation."[9]

It is clear that such a regime will require carefully crafted language to be politically feasible in addition to well-designed mechanisms capable of monitoring and verifying adherence and of cooperating when such incidents occur. And while the more ambitious option is more in sync with the rapidly deteriorating risk environment, it is rather out of sync with the conventional pace of diplomacy. The question is whether the evolution of the threat will keep pace with diplomacy or whether diplomacy will keep pace with the threat.

Focusing on Financial Stability: An Opportunity and a Necessity

Why should financial stability become a leading focus for the United States and China? Hackers certainly pose a growing risk to various critical infrastructure, so why focus on financial institutions? The key argument is that there is a higher degree of shared interest between the United States and China when it comes to the financial system, making international cooperation more feasible politically. The financial system is globally interdependent, and trust plays an important role for the system as a whole. While other types of infrastructure can be similarly critical to a nation, they are usually not globally interdependent.[10] In addition, they do not rely on trust. For example, in the context of the electrical grid, the lights are either on or off. The self-interest, and therefore the shared interest, in financial stability makes an agreement in this area politically more feasible and achievable than other similarly critical infrastructure and thus presents a more promising starting point.

Collaboration focusing on protecting global financial stability against cyber threats would build on the precedent of the 2015 US-China agreement regarding the "cyber-enabled theft of intellectual property" for "competitive advantages"—or economic espionage, in short.[11] It remains the single most important international cybersecurity agreement to date because it led to a measurable decrease in malicious activity coming from China,[12] a decrease confirmed by US government officials and private cyber threat intelligence companies alike.[13] At the same time, an agreement focusing on financial stability would be based on a different dynamic. It is no secret that the 2015 agreement was forged after significant and long-term pressure by the United States toward China building up over time.[14] Financial stability, on the other hand, is clearly a shared interest of both countries, one that they could rally behind on the international stage.

A second argument is the urgency of the threat. Cyber criminals, as well as nation-states, pose a growing risk to the global financial system. The timeline of cyber

incidents targeting financial institutions from 2007 to 2017 reveals that criminals have become more daring and that more nation-states have joined their ranks, targeting financial institutions for profit-driven and politically motivated purposes. The worrisome trend is the increasing number of nation-states using offensive cyber tools against financial institutions. Some states appear to target the financial system to make money, namely North Korea, which seems to have extended its efforts to try to prop up its state coffers by complementing its conventional counterfeiting of currency with large-scale cybercrime. Importantly, some nation-states have been targeting financial institutions not only to spy but to cause disruption and destruction, as illustrated by the massive distributed denial of service (DDoS) attacks by Iranian hackers against financial institutions in 2012.

Looking ahead, hackers can pose a risk to financial stability for different reasons. The most severe risk to the system's underlying trust consists of manipulations of the integrity of data and algorithms of financial institutions.[15] There are also certain choke points in the global financial system that, if they are unavailable intentionally or unintentionally for a certain period of time, could have a systemic effect. Previous conventional financial crises have illustrated that the source of contagion can come unexpectedly from small players. For example, the Asian financial crisis in 1997 was caused by the collapse of the Thai currency. At the time, conventional wisdom did not expect the collapse of the currency of a comparatively small player in the financial system, such as Thailand, to pose a significant risk, but its interdependence with Indonesia was underestimated, and once Indonesia was affected, the region became affected. Such contagion effects can also be triggered by the collapse of a single or a few institutions, as illustrated by the collapse of Lehman Brothers and its impact in 2007. Similar risks now exist in the computer architecture of the global financial system.

SELECTED CYBER INCIDENTS ILLUSTRATING GROWING RISK

- *2016 Bangladesh Central Bank Heist*
  In 2016, the media reported that hackers had breached the network of the Bangladesh central bank in an attempt to steal nearly $1 billion. The hackers ultimately succeeded in stealing "only" $81 million after a typo in their wiring instructions raised suspicion. The hackers had introduced malware onto the Bangladesh central bank's server and had deployed keylogger software that allowed them to steal the bank's credentials for the SWIFT system.[16]

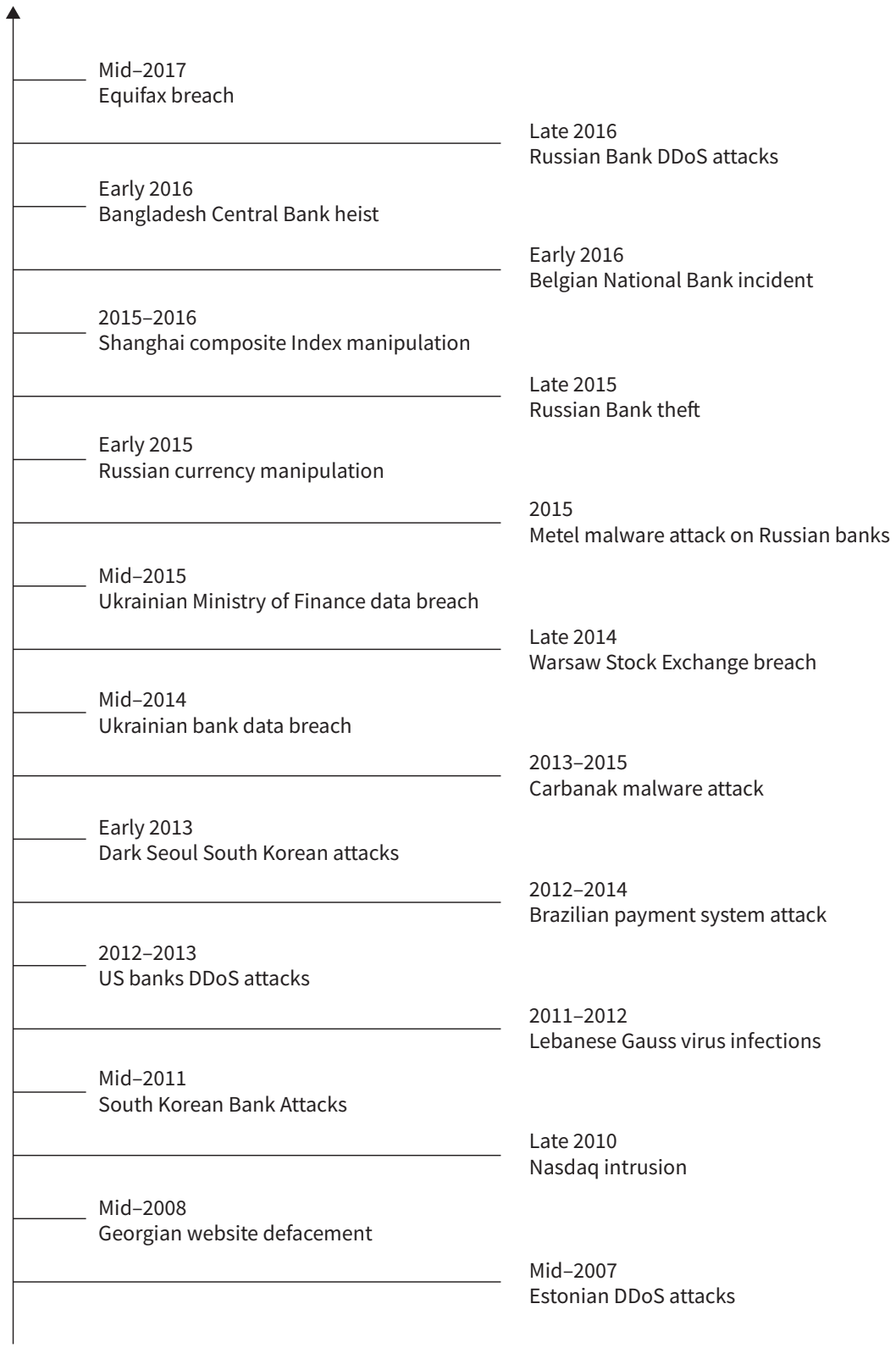
- *2013–2015 Carbanak Malware Attack on Various Banks*
  A group of criminals used Carbanak malware to attack financial institutions, including banks and electronic payment systems, in nearly thirty countries. The largest amounts of money were stolen when criminals impersonating bank officers hacked into the banks' accounting systems, manipulated account balances to inflate the amount of money available, and then transferred the additional money so that the balance then returned to the original amount.[17]

- *2013 Malware Attack on South Korean Banks*
  This attack on three South Korean banks—Shinhan, Nonghyup, and Jeju—resulted in data deletion and disruptions to ATMs and mobile payment systems. Shinhan Bank's internet banking servers were temporarily blocked for part of the day, leaving customers unable to perform online transactions, while operations at some branches of Nonghyup and Jeju were paralyzed for two hours after the virus erased files on the infected computers. A fourth bank, Woori, reported hacking but suffered no damage. South Korea attributed the attack to North Korea.[18]

- *2012–2014 Malware Attack on Brazilian Payment System*
  Cybercriminals used "man-in-the-browser" malware to target Boleto Bancário, a popular Brazilian payment system. The malware injected itself into browsers on nearly 200,000 infected computers, where it was able to intercept and alter legitimate boletos so as to route payments into the hackers' own accounts. The attack compromised $3.75 billion in transactions, although it is unclear how much of that money the criminals were able to successfully deposit into their own accounts.[19]

- *2012–2013 DDoS Attacks on US Financial Institutions*
  Two coordinated waves of DDoS attacks against US financial institutions' websites occurred in September–October 2012 and December 2012–January 2013. An Islamic "hacktivist" group called the Izz ad-Din al-Qassam Cyber Fighters claimed responsibility for the attacks, which they dubbed Operation Ababil, but US government officials have privately indicated to the media that they believe Iran is actually responsible. The scale of the attacks was unprecedented in the number of financial institutions hit and the amount of traffic flooding the sites.[20]

TIMELINE OF SELECTED CYBER INCIDENTS TARGETING FINANCIAL INSTITUTIONS (2007–2017)



Building on Nascent Efforts

Protecting financial institutions against these cyber threats has become a growing concern for governments around the world, from Beijing to Washington. In the United States, the government conducted exercises focusing specifically on the financial sector, and eight of the world's largest financial institutions created the Financial Systemic Analysis and Resilience Center.[21] In China, Beijing has been shifting the focus of its cybersecurity efforts since 2013 toward the protection of critical infrastructure, including the banking system. For example, China's new cybersecurity law, which entered into force in 2017, focused on financial institutions as "critical information infrastructure operators."[22] The debate about the new law illustrates Beijing's struggle to enhance the cybersecurity of its financial institutions without hurting their competitiveness and the openness of the market overall.

When the G20 Finance Ministers and Central Bank Governors acknowledged these new dark clouds on the horizon in their March 2017 communiqué, they not only recognized the risk but went a step further, taking a first step toward mitigating it:

> The malicious use of Information and Communication Technologies (ICT) could disrupt financial services crucial to both national and international financial systems, undermine security and confidence and endanger financial stability. We will promote the resilience of financial services and institutions in G20 jurisdictions against the malicious use of ICT, including from countries outside the G20. With the aim of enhancing our cross-border cooperation, we ask the FSB [Financial Stability Board], as a first step, to perform a stock-taking of existing relevant released regulations and supervisory practices in our jurisdictions, as well as of existing international guidance, including to identify effective practices. The FSB should inform about the progress of this work by the Leaders Summit in July 2017 and deliver a stock-take report by October 2017.[23]

This G20 communiqué followed several other notable policy developments in recent years. For example, in June 2016, the International Organization of Securities Commissions and the Committee on Payments and Market Infrastructures issued joint guidance on cyber resilience for financial market infrastructures.[24] A few months later, the G7 adopted the G7 Fundamental Elements of Cybersecurity for the Financial Sector.[25] And in addition to China's and the United States' aforementioned actions, other countries around the world set up or strengthened their computer emergency response teams (CERTs) specific to the financial sector, as, for example, India did in February 2017.[26] These initiatives are an important first step for taking

stock of existing best practices, assessing the current risk environment, and increasing resilience.

The Path Ahead

In the current climate of what one scholar has called a "new era of uncertainty,"[27] pragmatism and a focus on making progress in more narrowly defined areas of common interest are most likely to build trust and to advance the broader effort to mitigate risks and to develop rules of the road for cyberspace. A joint effort by the United States and China to protect financial stability would align with this approach. The 2015 agreement between the United States and China demonstrates how a bilateral agreement between the world's two largest economies can pave the way for such an agreement to be incorporated in the G20, which adopted similar language two months later.[28]

A useful starting point would be to add such an initiative to the agenda of the US-China Comprehensive Dialogue created in April 2017 following the first meeting of President Xi with President Trump.[29] The dialogue consists of four pillars:

- Diplomatic and Security Dialogue
- Comprehensive Economic Dialogue
- Law Enforcement and Cybersecurity Dialogue
- Social and Cultural Issues Dialogue

The Law Enforcement and Cybersecurity Dialogue took place for the first time in October 2017.[30] This is a promising development, as other parts of the Comprehensive Dialogue have stalled, namely the Comprehensive Economic Dialogue co-chaired by the US secretary of the Treasury, the US secretary of commerce, and their Chinese counterparts.[31] The latter has been stalled since November 2017 due to differences over the countries' trade and investment balance.[32]

As part of the Law Enforcement and Cybersecurity Dialogue, the two governments identified as one of four priorities of this dialogue "cybercrime and cybersecurity," specifically stating:

Both sides will continue their implementation of the consensus reached by the Chinese and American Presidents in 2015 on U.S.-China cybersecurity cooperation, consisting of the five following points:

(1) that timely responses should be provided to requests for information and assistance concerning malicious cyber activities;

(2) that neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors;

(3) to make common effort to further identify and promote appropriate norms of state behavior in cyberspace within the international community;

(4) to maintain a high-level joint dialogue mechanism on fighting cybercrime and related issues; and

(5) to enhance law enforcement communication on cyber security incidents and to mutually provide timely responses.

Both sides reiterated that all consensus and cooperative documents achieved at the three rounds of the China-U.S. High-Level Joint Dialogue on Combating Cyber Crimes and Related Issues since 2015 remain valid.

Both sides intend to improve cooperation with each other on cybercrime, including sharing cybercrime-related leads and information, and responding to Mutual Legal Assistance requests, in a timely manner, including with regard to cyber fraud (including business email compromises), hacking crimes, abuse of internet for terrorist purposes, and internet dissemination of child pornography.

Both sides will continue to cooperate on network protection, including maintaining and enhancing cybersecurity information sharing, as well as considering future efforts on cybersecurity of critical infrastructure.

Both sides intend to maintain and make full use of the established hotline mechanism for addressing urgent cybercrime and network protection issues pertaining to significant cybersecurity incidents, and to communicate in a timely way at the leadership level or working level, as needed.[33]

The Law Enforcement and Cybercrime Dialogue could, therefore, be the anchor for an initiative specifically focusing on protecting financial institutions against cyber threats. In fact, the more high-level commitments made in October 2017 could become operationalized in the specific context of malicious activity targeting financial institutions. In addition, the dialogue could serve as the incubator for a proposal that Beijing and Washington could take to the G20 for a broader agreement among the world's twenty largest economies.

The G20 would be a natural fit for such an agreement because it was created to focus on the global economy and because of the role it assumed in the wake of the 2007–2008 global financial crisis. The annual meetings of the G20 Finance Ministers and Central Bank Governors have since been complemented with meetings of the G20 heads of state. In addition, cybersecurity would not be a novel agenda item at the G20. In November 2015, the G20 heads of states included an entire paragraph dedicated to cybersecurity in their Antalya communiqué. In the words of Minister Wolfgang Schäuble, "The role that the G20 can play is to get governments of member states as much involved as possible. . . . It reminds me of times of Cold War when we needed cooperation. . . . The biggest problem in the global world can only be treated in a way that the major players find some way to compromise."[34]

Building on the 2015 report of the UN Group of Governmental Experts (UNGGE), namely the voluntary norm focusing on critical infrastructure, the March 2017 communiqué of the G20 Finance Ministers and Central Bank Governors, as well as the October 2017 outcome of the US-China Law Enforcement and Cybercrime Dialogue, the following paragraph could be integrated into a G20 communiqué in the future:

> The global financial system is highly interconnected, and an ICT-enabled incident in one nation can significantly affect the stability of the financial system in others. In recognition of this fact, the G20 finance ministers and central bank governors affirm that our nations will not accept any malicious use of ICT that could undermine security and confidence and endanger financial stability, such as by manipulating the integrity of data and algorithms of financial institutions or undermining the availability of critical financial systems. We will promote the resilience of financial services and institutions in G20 jurisdictions against the malicious use of ICT regardless of the origin of the threat. We will respond promptly to appropriate requests by another nation for assistance to prevent, mitigate, or respond if such malicious activity takes place, and we

> will cooperate with other nations to impose consequences on the perpetrator. We ask the FSB, as a next step, to act as a convener, bringing together its member jurisdictions, international financial institutions, and international standard-setting and other bodies as well as the private sector, the law enforcement, and Computer Emergency Response Team (CERT) communities to develop a road map for implementing this commitment. The FSB should inform about the progress of this work at the next Leaders Summit and deliver a stock-take report in the fall.

This proposed language is designed to establish the foundation for an effective international regime to protect financial stability against cyber threats based on three main pillars.[35]

The first pillar is the declaratory statement that states "will not accept any malicious use of ICT that could undermine security and confidence and endanger financial stability, such as by manipulating the integrity of data and algorithms of financial institutions or undermining the availability of critical financial systems."[36] This statement is meant to send a clear signal that the international community will not tolerate such behavior, building on the 2015 agreement focusing on economic espionage and the 2015 UNGGE norm on critical infrastructure.

The second pillar focuses on cooperation and pledges to "respond promptly to appropriate requests by another nation for assistance to prevent, mitigate, or respond if such malicious activity takes place" as well as to "cooperate with other nations to impose consequences on the perpetrator." This builds on the 2015 UNGGE report and seeks to operationalize the commitments in the specific context of the financial system. It also builds on the high-level commitments through the US-China Law Enforcement and Cybercrime Dialogue.

The third pillar centers on increasing resilience as the lever to build detection and monitoring systems to help identify when malicious incidents occur. Finally, governments are expected to adhere to the commitment included in the 2013 and 2015 UNGGE reports not to use proxies to circumvent such an agreement.

It is also worth highlighting that another advantage of an initiative focusing on the financial system is that some of the usual definitional challenges are less daunting when it comes to determining what is considered to be part of a commitment and what is excluded. First, whether the integrity of data has been manipulated is a

technical question that can be assessed. Second, there is widespread consensus that such manipulations constitute the most severe risk to a potential loss of trust in the system, partly explaining why there appears to have been significant restraint in this area. Meanwhile, the availability of critical systems is slightly more complicated because it requires an answer to what constitutes a "critical" system. However, following the intensive research conducted by governments around the world following the 2007–2008 global financial crisis assessing potential vulnerabilities and choke points in the system, there is now arguably a more sophisticated understanding of what systems and institutions are critical than ever before. This mitigates the risk of significant variations among governments of what constitutes "critical."

Building on 2015 Precedent

This proposed collaboration and joint initiative would build on the precedent set in 2015. The 2015 agreement between the United States and China shows that diplomacy and political commitments can be effective even in the new domain of cyberspace with its bits and bytes rather than warheads and missiles. It shows that changes in behavior can indeed be measured and monitored. A few years earlier, the report of the cybersecurity company Mandiant identifying a specific unit of the People's Liberation Army (PLA) involved in hacking already demonstrated that attributing malicious activity online is possible, though difficult.[37] A year later, the US government's indictment of five PLA officers made it clear that attribution can go as far as identifying the particular individuals involved.[38] The reported threat of sanctions by the White House also illustrates that enforcement is possible—in this case, the enforcement of the existing norm against economic espionage.[39] Finally, it shows that changes in behavior can occur without a binding instrument under international law but through high-level political commitments.

The United States and China, as the world's two largest economies, could lead the way for the international community to send a clear signal condemning cyberattacks targeting the financial system, namely those manipulating the integrity of financial institution data or undermining the availability of critical systems. Less than a handful of states have dared to violate this implicit understanding, namely North Korea and Iran. Issuing an explicit statement about this issue would send a powerful message about the international community's resolve and pave the way for more robust cooperation to tackle future malicious activity and threats. Such an initiative will not resolve the decade-old disagreements about the Convention on Cybercrime or how to define information/cybersecurity. Yet it provides an opening to create more

cooperation, at least for those incidents that could pose a risk to financial stability, potentially creating positive spillover effects for the broader discussions elsewhere.

China and the United States can also build on this precedent to further advance the international community's efforts to strengthen rules of the road for cyberspace. The global financial system, because of the common interest among states, is a promising area to implement some of the commitments made through the UNGGE process. Given the significant tensions and differences among the international community on many aspects relating to cybersecurity, including such foundational issues as the applicability of international law, a promising avenue to pursue is to focus on a more narrowly defined issue set to make further progress. This would help strengthen the more general existing umbrella agreement achieved through the UNGGE in 2015, namely the voluntary norm focusing on critical infrastructure.[40] Such an effort would also feed into whatever mechanism follows the UNGGE after the process collapsed in June 2017.[41]

Obstacles

A joint initiative between Beijing and Washington can only succeed under certain conditions. Obstacles include potential differing perceptions of risk regarding the financial system on either side of the Pacific. Such variation likely exists even within each government as their respective bureaucracies assess the new vulnerabilities and risks associated with the financial system's increasing digitization and interconnectness. This may further extend to perceptions of asymmetry: that one side might have a stronger interest in such an initiative and in protecting the financial system than the other. Beijing might care more because its overarching objective is regime stability; few scenarios spook Chinese leaders more than social unrest on the streets, such as that triggered by a run on the banks and financial instability. Washington might care more because it is the center of the global financial system; it has no appetite to put at risk its still-fragile recovery from the worst economic crisis since the 1930s. Other variables include the murky nature of China's banking industry and institutional versus network-layer connections.[42] Ultimately, it is clear that both countries have a vested interest in preserving and protecting financial stability at home and globally.

Another obstacle at the multilateral level is the lack of trust among several of the world's largest economies and most important political players, namely the United States, China, Russia, and European countries. These geopolitical tensions are reflected in various policy fields, including efforts to tackle cybercrime and discussions about

rules of the road and appropriate state behavior online. For example, while the Convention on Cybercrime has been in force since 2004, only fifty-six states have signed and ratified it today.[43] Several major states, such as China, Russia, Brazil, and India, continue to have reservations about joining the treaty. Brazil and India have opposed signing the convention, arguing that they didn't have a seat at the table when it was being negotiated through the Council of Europe. Russia and China see it as a potential infringement on their nation's sovereignty. It is unlikely that the dynamics of this decade-old debate will change significantly in the foreseeable future.

Similarly, while international discussions about appropriate state behavior made some progress through the UNGGE reports over the past few years, they have recently ground to a halt.[44] The future of this process remains uncertain. The 2013 UNGGE report was a milestone because it affirmed that high-level principles and instruments, namely sovereignty and international law, apply to cyberspace.[45] Sovereignty was important to China and Russia, in particular, and international law to the United States and European countries. The 2015 UNGGE report is significant because it includes a list of voluntary norms that could morph from being aspirational to actual standards of behavior.[46] Today, key differences remain among the major players. China and Russia continue to view cybersecurity through the broader lens of information security, considering content and the control of information to be part of this policy debate. The United States and other countries focus on cybersecurity through a more technical lens. A similar divide exists regarding the desired end goal. Beijing and Moscow have been promoting the idea of a comprehensive, legally binding treaty, whereas the United States and European countries have been pushing back against hard law instruments, focusing on norms through soft law instead.

Conclusion

Geopolitical tensions are on the rise worldwide, including between China and the United States. This will make multilateral cooperation and engagement generally, and diplomatic efforts focusing on more comprehensive frameworks specifically, more challenging. At the same time, the technological change will persist, transforming societies that become increasingly digitally connected in terms of both humans and machines. Governments can either manage emerging risks associated with this transformation proactively or respond reactively to them after major incidents. Some of these risks have a systemic dimension requiring particular attention. This includes the financial system, and clear warning signs are already on the horizon. The United States and China have an opportunity to proactively mitigate these risks given their

shared interest and their combined influence. Cooperating in this more narrowly defined area holds greater promise in the current political environment than more ambitious initiatives do. The initiative outlined in this paper could be the blueprint for such a joint endeavor when the political window of opportunity presents itself.

Acknowledgments

I thank Kamaal Thomas and Travis Hahn for their research assistance with this paper. I also thank George Perkovich, Ben Wittes, and a Chinese scholar, who prefers to remain anonymous, for their feedback and comments.

NOTES

1 White House, "Presidential Memorandum on the Actions by the United States Related to the Section 301 Investigation," March 22, 2018, accessed May 24, 2018, https://www.whitehouse.gov/presidential-actions/presidential-memorandum-actions-united-states-related-section-301-investigation.

2 Jeremy Diamond, "Trump Hits China with Tariffs, Heightening Concerns of Global Trade War," CNN, March 23, 2018, accessed May 24, 2018, https://www.cnn.com/2018/03/22/politics/donald-trump-china-tariffs-trade-war/index.html.

3 Michael Corkery and Matthew Goldstein, "North Korea Said to Be Target of Inquiry over $81 Million Cyberheist," *New York Times*, March 22, 2017, accessed May 24, 2018, https://www.nytimes.com/2017/03/22/business/dealbook/north-korea-said-to-be-target-of-inquiry-over-81-million-cyberheist.html.

4 "WannaCry ransomware attack," *Wikipedia*, last modified February 4, 2018, https://en.wikipedia.org/wiki/WannaCry_ransomware_attack; Russell Brandom, "UK Hospitals Hit with Massive Ransomware Attack," *The Verge*, May 12, 2017, accessed May 24, 2018, https://www.theverge.com/2017/5/12/15630354/nhs-hospitals-ransomware-hack-wannacry-bitcoin.

5 "Communiqué," Finance Ministers and Central Bank Governors Meeting, G20, March 17–18, 2017, accessed May 24, 2018, http://carnegieendowment.org/files/g20-communique.pdf.

6 Other experts have made similar arguments in the past. A working group on foreign policy and grand strategy at Stanford University's Hoover Institution argued in December 2015 that "the United States must work to develop international norms against cyber acts of mass disruption. The best place to start is working with China to develop a formalized arrangement to protect global financial systems, an issue on which China and the United States have strong shared interests." Amy Zegart and Stephen D. Krasner, eds., "Pragmatic Engagement amidst Global Uncertainty: Three Major Challenges," Hoover Institution, December 11, 2015, accessed May 24, 2018, https://www.hoover.org/research/pragmatic-engagement-amidst-global-uncertainty-three-major-challenges. See also Richard A. Clarke and Robert K. Knake, *Cyber War* (CITY: Ecco, 2011).

7 Noah Bierman and Brian Bennett, "Trump and China's President Xi Form a Personal Bond, but Will It Yield Trump's Promised Deals?," *Los Angeles Times*, November 7, 2017, accessed May 24, 2018, http://www.latimes.com/politics/la-na-pol-trump-xi-20171107-story.html.

8 Tim Starks, "Top White House Official Talks Cyber Command, International Engagement, More," *Politico*, July 21, 2017, accessed May 24, 2018, https://www.politico.com/tipsheets/morning-cybersecurity/2017/07/21/top-white-house-official-talks-cyber-command-international-engagement-more-221454.

9 Adam Segal, "Chinese Cyber Diplomacy in a New Era of Uncertainty," Hoover Working Group on National Security, Technology, and Law, Aegis Paper Series No. 1703, June 2, 2017, accessed May 24, 2017, https://www.hoover.org/sites/default/files/research/docs/segal_chinese_cyber_diplomacy.pdf.

10 The internet is arguably the only other infrastructure that is similarly globally interdependent and as reliant on trust, e.g., when it comes to its certificate and other authentication systems.

11 Office of the Press Secretary, White House, "Fact Sheet: President Xi Jinping's State Visit to the United States," September 25, 2015, accessed May 24, 2018, https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.

12 Recent reports suggest that there has been an increase in malicious activity, but it is not clear whether it is actually violating the agreement and an attempt to send a signal to the new administration, focusing on potential dual-use technologies that fall into a gray zone, or actions by potential rogue actors. Adam Segal, "An Update on U.S.-China Cybersecurity Relations," *Net Politics* (blog), Council on Foreign Relations, November 17, 2017, accessed May 24, 2018, https://www.cfr.org/blog/update-us-china-cybersecurity-relations.

13 "Senate Armed Services Committee-Hearing Subject: U.S. Cyber Command Witnesses: Navy Adm. Michael Rogers, Commander of the U.S. Cyber Command, Director of the National Security Agency and Chief of Central Security Services, Testify," C-SPAN (video), April 5, 2016, accessed May 24, 2018, https://www.c-span.org/video/?407662-1/hearing-us-cyber-command-operations; "Red Line Drawn: China Recalculates Its Use of Cyber Espionage," FireEye, June 20, 2016, accessed May 24, 2018, https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf.

14 Segal, "Chinese Cyber Diplomacy."

15 Joel Brenner, "Keeping America Safe: Toward More Secure Networks for Critical Sectors" (MIT Center for International Studies, March 2017), accessed May 24, 2018, http://carnegieendowment.org/files/MITReport-IPRI-CIS-CriticalInfrastructure-2017-Brenner.pdf.

16 Steve Herman, "Historic Bangladesh Bank Heist Muddled in Mystery," Voice of America, March 24, 2016, http://www.voanews.com/content/historic-bangladesh-bank-heist-muddledin-mystery/3252379.html; Rick Gladstone, "Bangladesh Bank Chief Resigns After Cyber Theft of $81 Million," *New York Times*, March 15, 2016, http://www.nytimes.com/2016/03/16/world/asia/bangladesh-bank-chief-resigns-after-cyber-theft-of-81-million.html?_r=0; Reuters, "Spelling Mistake Prevented Hackers Taking $1bn in Bank Heist," *Guardian*, March 10, 2016, http://www.theguardian.com/business/2016/mar/10/spelling-mistake-prevented-bank-heist; Sergei Shevchenko, "Two Bytes To $951m," *Bae Systems Threat Research Blog*, April 25, 2016, http://baesystemsai.blogspot.com/2016/04/two-bytes-to-951m.html

17 Kaspersky Lab's Global Research and Analysis Team, "The Great Bank Robbery: The Carbanak APT," *Securelist* (blog), Kaspersky Lab, February 16, 2015, https://securelist.com/blog/research/68732/the-great-bank-robbery-the-carbanak-apt/

18 Choe Hang-Sun, "Computer Networks in South Korea Are Paralyzed in Cyberattacks," *New York Times*, March 20, 2013, http://www.nytimes.com/2013/03/21/world/asia/south-koreacomputer-network-crashes.html; Juan C. Zarate, "The Cyber Financial Wars on the Horizon," Foundation for Defense of Democracies, July 2015, http://www.defenddemocracy.org/content/uploads/publications/Cyber_Financial_Wars.pdf, 12–13; Hang-Sun, "Computer Networks in South Korea," *New York Times;* K.J. Kwon, "Smoking Gun: South Korea Uncovers Northern Rival's Hacking Codes," CNN, April 22, 2015, http://www.cnn.com/2015/04/22/asia/koreas-cyber-hacking/

19 Robert Lemos, "Cyber-Attacks Seen Defrauding Brazilian Payment System of Billions," *eWeek*, July 6, 2014, http://www.eweek.com/security/cyber-attacks-seen-defrauding-brazilian-payment-systemof-billions.html; Eli Marcus, "RSA Uncovers Boleto Fraud Ring in Brazil," RSA, July 2, 2014, https://blogs.rsa

.com/rsa-uncovers-boleto-fraud-ringbrazil/; "Boleto Malware May Lose Brazil $3.75bn," BBC, July 3, 2014, http://www.bbc.com/news/technology-28145401

20 Emilio Iasiello, "Cyber Attack: A Dull Tool to Shape Foreign Policy" (paper presented at the 2013 5th International Conference on Cyber Conflict), 11, https://ccdcoe.org/cycon/2013/proceedings/d3r1s3_Iasiello.pdf; David Goldman, "Major Banks Hit With Biggest Cyberattacks in History," CNN, September 28, 2012, http://money.cnn.com/2012/09/27/technology/bank-cyberattacks/; Barbara Slavin, "US Withholds Evidence for Iran Cyberattacks," *Al-Monitor*, January 17, 2013, http://www.al-monitor.com/pulse/originals/2013/01/cyber-attacks-us-iran-ddos.html; Nicole Perlroth and Quentin Hardy, "Bank Hacking Was the Work of Iranians, Officials Say," *New York Times*, January 8, 2013, http://www.nytimes.com/2013/01/09/technology/online-bankingattacks-were-work-of-iran-us-officials-say.html.

21 Shaun Waterman, "Bank Regulators Briefed on Treasury-Led Cyber Drill," FedScoop, July 20, 2016, accessed May 24, 2018, https://www.fedscoop.com/us-treasury-cybersecurity-drill-july-2016; Financial Services Information Sharing and Analysis Center, "FS-ISAC Announces the Formation of the Financial Sytemic Analysis and Resilience Center," news release, October 24, 2016, accessed May 24, 2018, https://www.fsisac.com/sites/default/files/news/FS-ISAC%20Announces%20the%20Formation%20of%20the%20Financial%20Systemic%20Analysis%20%28FSARC%29.pdf.

22 Kareena Teh and Philip Kwok, "China Cybersecurity Law: Key Takeaways for Financial Services Firms in China," Dechert LLP, June 26, 2017, accessed May 24, 2018, https://info.dechert.com/27/8822/landing-pages/china-cybersecurity-law—key-takeaways-for-financial-services-firms-in-china.asp.

23 "Communiqué," Finance Ministers and Central Bank Governors Meeting.

24 Committee on Payments and Market Infrastructures, and Board of the International Organization of Securities Commissions, Bank for International Settlements, "Guidance on Cyber Resilience for Financial Market Infrastructures," BIS, June 29, 2016, accessed May 24, 2018, https://www.bis.org/cpmi/publ/d146.htm.

25 G7 Cyber Expert Group, "G7 Fundamental Elements of Cybersecurity for the Financial Sector," October 11, 2016, accessed May 24, 2018, https://www.fin.gc.ca/n16/docs/g7-1014-eng.pdf.

26 Sandhya Dangwal, "Computer Emergency Response Team to Be Set Up to Check Cyber Frauds," India, February 1, 2017, accessed May 24, 2018, http://www.india.com/news/india/budget-2017-computer-emergency-response-team-to-be-set-up-to-check-cyber-frauds-1802854.

27 Segal, "Chinese Cyber Diplomacy."

28 Office of the Press Secretary, "Fact Sheet"; "G20 Leaders' Communiqué," Finance Ministers and Central Bank Governors Meeting, G20 Turkey Summit, November 15–16, 2015, accessed May 24, 2018, http://www.g20.utoronto.ca/2015/151116-communique.pdf.

29 Office of the Press Secretary, White House, "Statement from the Press Secretary on the United States-China Visit," April 7, 2017, accessed May 24, 2018, https://www.whitehouse.gov/briefings-statements/statement-press-secretary-united-states-china-visit.

30 Office of Public Affairs, US Department of Justice, "First U.S.-China Law Enforcement and Cybersecurity Dialogue," news release, October 6, 2017, accessed May 24, 2018, https://www.justice.gov/opa/pr/first-us-china-law-enforcement-and-cybersecurity-dialogue.

31 "U.S.-China Comprehensive Economic Dialogue," US Department of the Treasury, last modified June 26, 2017, accessed May 24, 2018, https://www.treasury.gov/initiatives/Pages/china.aspx.

32 Sam Fleming and Shawn Donnan, "Trump Puts Talks to Boost China Economic Ties on Ice," *Financial Times*, November 30, 2017, accessed May 24, 2018, https://www.ft.com/content/469d99c0-d5ee-11e7-8c9a-d9c0a5c8d5c9.

33 Office of Public Affairs, US Department of Justice, "First U.S.-China Law Enforcement and Cybersecurity Dialogue."

34 Carnegie Live, "German Finance Minister Wolfgang Schäuble on G20 Priorities and Transatlantic Relations," YouTube (video), 28:30, April 20, 2017, accessed May 24, 2018, https://www.youtube.com/watch?v=VtcMd5QLgMA&feature=youtu.be&t=1710.

35 In March 2017, the Carnegie Endowment for International Peace published a report titled "Toward a Global Norm against Manipulating the Integrity of Financial Data" proposing a G20 agreement focusing on cybersecurity and financial stability, including specific suggestions for normative language. This proposal can be tailored to focus specifically on implementing the UNGGE commitments in the context of the financial system, which is the basis for the approach taken in this essay.

36 An open question is whether this would apply in peacetime and in wartime. The Carnegie Endowment proposal does not distinguish between the two. Focusing specifically on armed conflict, Michael Schmitt and Tim Maurer coauthored an article discussing the importance in the context of how international humanitarian law applies specifically with regard to the integrity of data. One approach, as implied by the proposed draft language, is not to specify this point at first but to explore its applicability during armed conflict over time and to clarify states' interpretation through unilateral or complementary multilateral statements down the road. Michael Schmitt and Tim Maurer, "Protecting Financial Data in Cyberspace: Precedent for Further Progress on Cyber Norms?," *Just Security*, August 24, 2017, accessed May 24, 2018, https://www.justsecurity.org/44411/protecting-financial-data-cyberspace-precedent-progress-cyber-norms.

37 Mandiant, "APT1: Exposing One of China's Cyber Espionage Units," FireEye, February 18, 2013, accessed May 24, 2018, https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf.

38 Office of Public Affairs, US Department of Justice, "U.S. Charges Five Chinese Military Hackers for Cyber Espionage against U.S. Corporations and a Labor Organization for Commercial Advantage," news release, May 19, 2014, accessed May 24, 2018, https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

39 Julie Hirschfeld Davis, "Obama Hints at Sanctions against China over Cyberattacks," *New York Times*, September 16, 2015, accessed May 24, 2018, https://www.nytimes.com/2015/09/17/us/politics/obama-hints-at-sanctions-against-china-over-cyberattacks.html?mtrref=www.google.com&gwh=59D56C08A9B000EC8D57D69AC7CC42B0&gwt=pay.

40 "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," United Nations General Assembly, July 22, 2015, accessed May 24, 2018, http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.

41 After the failure of the UN Group of Governmental Experts (UNGGE) to adopt a consensus report in June 2016, the two-decade-old process at the United Nations has come to a halt and is currently in a "gap year" phase. It is unclear if the process will be resumed and, if so, how, whether through another UNGGE, a new open-ended working group, or a transfer to an existing body. Adam Segal, "The Development of Cyber Norms at the United Nations Ends in Deadlock. Now What?," *Net Politics* (blog), Council on Foreign Relations, June 29, 2017, accessed May 24, 2018, https://www.cfr.org/blog/development-cyber-norms-united-nations-ends-deadlock-now-what.

42 Bryan Borzykowski, "Trade War with US Could Be the Tipping Point for China's $14 Trillion Debt-Ridden Economy," CNBC, April 24, 2018, accessed May 24, 2018, https://www.cnbc.com/2018/04/24/trade-war-with-us-may-be-tipping-point-for-chinas-debt-ridden-economy.html.

43 "Chart of Signatures and Ratifications of Treaty 185," Treaty Office, Council of Europe, last modified February 5, 2018, accessed DATE, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=s3a2NnMw.

44 Segal, "Development of Cyber Norms at the United Nations."

45 "Report of the Group of Governmental Experts."

46 "Report of the Group of Governmental Experts."

The preferred citation for this publication is Tim Maurer, *The Case for Pragmatism and an Opportunity for Sino-US Leadership: Protecting Financial Stability Against Cyber Threats*, Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper No. 1808 (June 20, 2018), available at https://lawfareblog.com/case-pragmatism-and-opportunity-sino-us-leadership-protecting-financial-stability-against-cyber.

About the Author

TIM MAURER

Tim Maurer is the codirector of the Cyber Policy Initiative at the Carnegie Endowment for International Peace. Since 2010, his work has been focusing on cybersecurity, human rights in the digital age, and internet governance, currently with a specific focus on cybersecurity and financial stability. In January 2018, Cambridge University Press published his *Cyber Mercenaries: The State, Hackers, and Power.*

Working Group on National Security, Technology, and Law

The Working Group on National Security, Technology, and Law brings together national and international specialists with broad interdisciplinary expertise to analyze how technology affects national security and national security law and how governments can use that technology to defend themselves, consistent with constitutional values and the rule of law.

The group focuses on a broad range of interests, from surveillance to counterterrorism to the dramatic impact that rapid technological change—digitalization, computerization, miniaturization, and automaticity—are having on national security and national security law. Topics include cybersecurity, the rise of drones and autonomous weapons systems, and the need for—and dangers of—state surveillance. The group's output will also be published on the Lawfare blog, which covers the merits of the underlying legal and policy debates of actions taken or contemplated to protect the nation and the nation's laws and legal institutions.

Jack Goldsmith and Benjamin Wittes are the cochairs of the National Security, Technology, and Law Working Group.

For more information about this Hoover Institution Working Group, visit us online at http://www.hoover.org/research-teams/national-security-technology-law-working-group.

Hoover Institution, Stanford University
434 Galvez Mall
Stanford, CA 94305-6003
650-723-1754

Hoover Institution in Washington
The Johnson Center
1399 New York Avenue NW, Suite 500
Washington, DC 20005
202-760-3200

HOOVER INSTITUTION