A HOOVER INSTITUTION ESSAY

Chinese Cyber Diplomacy in a New Era of Uncertainty

ADAM SEGAL

Aegis Paper Series No. 1703

After initially taking a relatively defensive, reactive position on the global governance of cyberspace, China under President Xi Jinping has adopted a more activist cyber diplomacy. This foreign policy has three primary goals: limit the threat that the Internet and the flow of information may pose to domestic stability and regime legitimacy; shape cyberspace to extend Beijing's political, military, and economic influence; and counter US advantages in cyberspace while increasing China's room to maneuver. In effect, Beijing is pursuing a parallel track of managing state-to-state interactions along with efforts to generate international norms that reinforce and support domestic controls on information and data.

Like its efforts in more traditional areas of foreign policy, Chinese cyber diplomacy is rooted in noninterference in internal affairs, equal participation, development assistance and capacity building, and support for the United Nations and other multilateral institutions.[1] The linchpin of China's efforts is the idea of cyber (or Internet) sovereignty. As described by President Xi at the 2015 World Internet Conference in Wuzhen, cyber sovereignty means "respecting each country's right to choose its own Internet development path, its own Internet management model, [and] its own public policies on the Internet." The first principle listed in the 2016 national cyberstrategy is "respecting and protecting sovereignty in cyberspace." The first strategic task is to "resolutely defend sovereignty in cyberspace" and "oppose all actions to subvert our country's national regime or destroy our country's sovereignty through the network."[2] While sovereignty in cyberspace is not an inherently revisionist idea—the first and second editions of the Tallinn Manual note, for example, "A State may exercise control over cyber infrastructure and activity within its sovereign territory"—this position has been held out in contrast to the vision of cyberspace as an open, global platform held by the United States and its partners.[3]

Cyber sovereignty may be at the center of much of China's cyber diplomacy, but Beijing has also used commercial diplomacy and participation in international technical standards to shape cyberspace for economic and political interests. Moreover, cyber diplomacy is part of Beijing's efforts to contain the risk of terrorism, consolidate

its regional influence, and manage its bilateral relationships with the United States and other important partners.

In the near term, Chinese cyber policy will be shaped by—and will need to react to—two external shifts. First, as with other areas of foreign policy, a more inward-looking United States may create opportunities for China to play an even larger role in defining the rules of the international order in cyberspace. The Trump administration's cybersecurity executive order states that it is US policy to "promote an open, interoperable, reliable, and secure Internet." But abandoning free trade agreements and weakening alliance relationships will significantly undermine Washington's ability to pursue its goals in cyberspace.[4] With populist and antiglobalization sentiment growing in most Western economies, data nationalism may become an even more pronounced force. China may be able to exploit these sentiments diplomatically.

It is also very likely that the Trump administration will not vocally criticize China's control of its domestic Internet. The Trump administration's foreign policy has been characterized as "transactional nationalism," rooted in getting the best deals and protecting American interests, but not promoting American values.[5] Although the State Department reported that Secretary Rex Tillerson raised human rights with his hosts on a March 2017 visit to Beijing, the headline of his meeting with Xi was a repetition of Chinese diplomatic calls for a relationship based on the "principle of no conflict, no confrontation, mutual respect, and win-win cooperation."[6]

The Trump administration will not carry forward the banner of the Internet freedom agenda. An early draft of the cybersecurity executive order contained a section on "Internet Freedom and Governance," with a recommendation for producing a report for the president on actions supporting the multi-stakeholder process, but it was edited out of the final version.[7] Criticism of Chinese censorship and filtering would be moot at best, removing a major source of irritation for Beijing. If the two sides are not engaged in a trade war (or a standoff over Taiwan or the South China Sea), China may believe that it can partner with the United States on combating cyberterrorism and controlling rumors and "fake news."

Second, Beijing may face an even more dangerous cybersecurity environment. China may be worried that Russia's hacking of the Democratic National Committee and the US response will accelerate the "militarization" of cyberspace. It may even fear that it will be caught in the fallout if a conflict breaks out. In March 2017, the Ministry

of Foreign Affairs and the Cyberspace Administration of China jointly issued the International Strategy of Cooperation on Cyberspace.[8] The International Strategy lists the principle of peace before sovereignty. The first steps in China's plan of future action include bilateral and multilateral discussions on confidence-building measures and work with others to prevent an arms race in cyberspace.

Cyber Sovereignty

From the moment that China first connected to the Internet, Chinese policymakers and analysts saw cyberspace as a double-edged sword—essential to economic growth and good governance but also a threat to domestic stability and regime legitimacy. Given this sensitivity to internal threats, Chinese policymakers have typically referred to "information security" as opposed to cybersecurity. For American and European officials, "cybersecurity" generally means protecting communications and other critical networks from unauthorized access. For Chinese policymakers, like their Russian counterparts, information security is a much broader category that includes controlling the flow of information and censoring content as well as defending networks and computers from exploitation.

China addressed these concerns primarily through domestic laws and the deployment of filtering and censorship technologies widely known as the Great Firewall. At the international level, Beijing argued that cooperation must be based on mutual respect and the recognition of distinct national conditions. The 2010 Internet White Paper, for example, framed international cooperation in terms of national differences: "National situations and cultural traditions differ among countries, and so concern about Internet security also differs. . . . We should seek common ground and reserve differences, promote development through exchanges, and jointly protect international Internet security." The white paper also declared, "Within Chinese territory the Internet is under the jurisdiction of Chinese sovereignty. The Internet sovereignty of China should be respected and protected."[9]

Beijing's cyber diplomacy was also focused on what Chinese leaders and analysts saw as the uneven distribution of Internet resources, American control of the Internet Assigned Numbers Authority (IANA), and the contract with the Internet Corporation for Assigned Names and Numbers (ICANN). The Chinese press often complained that ten of the world's thirteen root servers were located in the United States and that the contract for the IANA process was between ICANN and the US Department of Commerce.[10] As the scholar Lu Chuanying describes it, "The US had practically

complete control over formulating and managing the Internet standards of all international organizations and core industries, and it refused to internationalize relevant functions and management or cede authority to a specialized UN agency to manage."[11]

In response to this perceived US domination, China, for example, called for the replacement of the multi-stakeholder model of governance with an International Internet Treaty and the formation of an Intergovernmental Internet Organization in 2003 at a preparatory meeting for the first World Summit on the Information Society.[12] The 2010 white paper also reasserted the importance of the United Nations: "China holds that the role of the U.N. should be given full scope in international Internet administration."

While Beijing often defended its Internet practices from outside criticism, it was the promotion of what was known as the Internet freedom agenda by the United States, as well as the release of the White House International Strategy for Cyberspace and the Pentagon's first cyberstrategy document, which created a growing apprehension that Washington was trying to contain China in cyberspace. Between 2010 and 2011, Secretary of State Hillary Clinton delivered three speeches on Internet freedom, asserting the freedom of expression and religion online, as well as the freedom to access the Internet and thereby to connect to websites and other people. In her January 2010 speech, Clinton criticized China for walling itself off from "the progress of the next century" and promised that the United States would develop and distribute technologies to help people avoid censorship.[13] Beijing reacted to these speeches defensively, interpreting them as directed at China's political system. "The United States," said one article in the *People's Daily,* "applies double standards in implementing freedom of information: for those who have different political views or values, it waves a 'freedom fighter's' club and leads a crusade against them."[14]

The May 2011 International Strategy for Cyberspace generated a similar set of negative responses from Chinese commentators. The Chinese press saw the strategy as a cover for the development of offensive capabilities, the "militarization" of cyberspace, and continued dominance by US technology companies. Two months later, in July 2011, the Department of Defense published its Strategy for Operating in Cyberspace. A number of prominent analysts argued that not only was the United States gaining diplomatic momentum in cyberspace, but also that China lacked a comprehensive strategy linking the diplomatic, military, and technological components of cyberspace.

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. The submission happened two months before the London Conference, a United Kingdom-sponsored attempt to identify norms of state behavior, and may have been in part an attempt to blunt the diplomatic efforts of the United States and its allies. 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 also reaffirmed "that policy authority for Internet-related public issues is the sovereign right of States, which have rights and responsibilities for international Internet-related public policy issues."[15]

The code was submitted to the United Nations again in 2015 by the Shanghai Cooperation Organization (SCO), the Eurasian regional organization that includes China, Russia, Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan.[16] Supporters of this revised version may have hoped to take advantage of the political fallout from NSA contractor Edward Snowden's disclosure of classified information, garnering support for new norms of information security from other states threatened by the surveillance conducted by the United States and its Five Eyes partners. The new version also shifted the debate on international human rights.[17] The 2011 version of the code allowed for restrictions based on "relevant national laws and regulations." The later code replaced national standards with an international basis, citing limits allowed under the International Covenant on Civil and Political Rights (ICCPR). Such a shift might have been attractive to states who wanted to be seen as upholding international law, even if that interpretation is inconsistent with the application of the ICCPR.

State Norms and the Group of Government Experts

In the years after the Clinton speech, the experience and sophistication of the Chinese participants in the UN Group of Government Experts (GGE) on the Developments in the Field of Information and Telecommunications in the Context of International Security increased. The United Nations first began considering issues of cybersecurity after Russia submitted in 1998 a draft resolution to the First Committee of the UN General Assembly (Disarmament and International Security Committee). The First Committee established the first group of cyber experts in 2004. The group has convened five times since. China was a passive participant at the earlier round of GGE meetings, which one US official characterized as "acting like a back bencher." Chinese

representatives at the 2004–05 meetings, for example, came from the Ministry of Communications, not the Foreign Ministry. In 2009, however, the United States started making some progress on promoting international law in cyberspace. In a late round of discussions, China sent a more seasoned diplomat.

The first and second meetings of the GGE failed to find any common ground. In June 2013, for the first time, the GGE came to a consensus. The members of the group, which included representatives from China, Russia, the United States, and twelve other nations, agreed that "international law, and in particular, the United Nations Charter, applies to cyberspace." The report also stated that "State sovereignty and international norms and principles that flow from sovereignty apply to State conduct."[18] US 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.

China's willingness to sign on to the 2012–13 consensus appears to have been less conscious diplomatic decision and more unplanned outcome. China's representatives in the early rounds were lower-level Ministry of Foreign Affairs officials with little experience with cyber issues. The final discussions on the report overlapped with President Xi Jinping's meeting with President Obama at the Sunnylands estate in Rancho Mirage, California. By some accounts, the Chinese representative signed because she was afraid that a story of Chinese intransigence would show up in the media and overshadow the summit.

Coming out of the 2012–13 GGE, Chinese officials highlighted the GGE's embrace of state authority, not the international law implications of accepting the UN Charter's application to cyberspace. In late 2013, for example, Lu Wei, who was then head of China's State Internet Information Office, began promoting sovereignty as central to China's view of cyberspace and as the basis for international cooperation. Speaking to the Second China-South Korea Internet Roundtable in December, Lu spoke of the need to safeguard network security sovereignty. Sovereignty, in Lu's conception, was an evolving concept. Just as the seventeenth century saw the extension of national sovereignty over parts of the sea, and the twentieth over airspace, national sovereignty is now being extended to cyberspace. Information services could cross borders, "but cyberspace cannot live without sovereignty."[19]

Other officials further developed the idea of sovereignty, stressing authority, noninterference, and equality. Numerous Chinese policymakers have noted that states

have jurisdiction over the ICT infrastructure and activities within their territories, and so are entitled to make public policies for the Internet based on their national conditions. Chinese diplomats also stress that governments should not use the Internet to interfere in countries' internal affairs. Moreover, states should participate in the governance of cyberspace as equals, building a global Internet governance system that is fair and equitable, based on the "principles of multilateralism, democracy and transparency."

The 2014–15 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 [ICT] by States." Beijing began sending much more experienced diplomats to the GGE, ambassador-level officials with experience in arms control negotiations. China, along with Russia, worked during 2015 to protect and expand the statement of the sovereignty norm. Like the 2013 report, the final report said, "State sovereignty and international norms and principles that flow from sovereignty apply to the conduct by States of ICT-related activities and to their jurisdiction over ICT infrastructure within their territory."[20] But the 2015 report included an additional section, "How international law applies to the use of ICTs," which further develops these ideas, noting that "States must observe, among other principles of international law, State sovereignty, sovereign equality, the settlement of disputes by peaceful means and non-intervention in the internal affairs of other States."

Beijing and Moscow signed off on four norms promoted by Washington in the 2015 report. The report promoted a norm of state responsibility and duty to assist as well as the idea 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 UN Charter, which authorizes the use of force in self-defense against an "armed attack."[21] Chinese analysts have typically argued that such a move would "militarize" cyberspace.[22] They also fear that the United States would use international law as justification to launch retaliatory strikes for cyberespionage.

China and Russia also used the GGE to express concern about the increasing willingness of the United States to name and shame state-backed hackers. During the two years between the 2013 and 2015 reports, Washington called out Beijing

for cyber industrial espionage; indicted five People's Liberation Army (PLA) hackers; and levied sanctions against North Korea in retaliation for hacking Sony Pictures. In all of these cases, attribution included a mix of private security company reports and US government releases of threat information and attack data. While the US government has gradually argued that it is getting better at attribution, the Chinese government has been consistent that such efforts often are "unprofessional" and "unscientific."[23]

The 2014–15 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." China's 2017 international strategy echoes this concern, arguing that since "cyberattacks are usually transnational and difficult to attribute, countries should work together to ensure cybersecurity through constructive consultation and cooperation."[24]

Going into the 2016–17 GGE meetings, US officials have called for the adoption of existing rules and confidence-building measures, not the identification of new norms. "We don't need a continual norms machine ramping out a lot of norms," said State Department deputy coordinator for cyber issues Michele Markoff. "What we need to do is consolidate what we've done and get states to implement."[25] While US diplomats have noted that China and Russia are unwilling to discuss any further how international law applies in cyberspace, and instead want to shift conversations to the need for a new treaty covering cyber norms, the 2017 International Strategy says China will "encourage the international community to discuss the peaceful nature of cyberspace and study the application of international law in cyberspace."

World Internet Conference

The UN has not been the only forum for the development of international norms. The London Conference has become such a process, with follow-up meetings in Seoul and The Hague. Situated midway between multilateral discussions at the United Nations and the multi-stakeholder approach of the Internet Governance Forum, these events have tended to be dominated by the United States and like-minded countries and have included discussions about online rights and the economic benefits of the open Internet.

The proliferation of these and other cyber discussions spurred Beijing's own policy entrepreneurship. In November 2014, China held its first World Internet Conference in Wuzhen, a historic town near Hangzhou, home to the headquarters of the Alibaba Group. The event, which was organized by the Cyberspace Administration of China, was meant as a showcase for the Chinese Internet economy and as a forum to promote Beijing's vision of the governance of cyberspace. In a prepared statement read by Vice Minister Ma at the opening, President Xi called for a "multifaceted, democratic and transparent governance system for the international Internet."[26]

While the organizers hoped to turn the event into a showcase for Chinese Internet companies, the Western press tended to focus on the incongruity of Facebook, Twitter, and other sites usually blocked within China being available in Wuzhen. The conference also made headlines for a diplomatic misstep.[27] The night before the closing ceremony, organizers slipped a draft document under participants' doors asking them to sign off. The document contained nine points, which included encouraging joint efforts on cybersecurity and fighting cyberterrorism, developing the Internet economy, and enhancing connectivity. It also called for respect for the Internet sovereignty of all countries. Many of the participants, however, balked at signing, and the conference ended with no final declaration.

If the first year was a test run, China signaled the political and diplomatic importance of the World Internet Conference by having Xi deliver the opening comments in person at the second Wuzhen conference in 2015. In his comments, Xi argued that all should "respect the right of individual countries to independently choose their own path of cyber development, model of cyber regulation and Internet public policies, and participate in international cyberspace governance on an equal footing." "No country," he continued, "should pursue cyber hegemony, interfere in other countries' internal affairs or engage in, connive at or support cyber activities that undermine other countries' national security."[28] Xi also criticized the global governance of the Internet, which he said failed to "reflect the desires and interests of the majority of countries." Xi did not mention specific institutions but stressed that governance should feature "a multilateral approach with multi-party participation."

China did also try to co-opt some of the energy of the multi-stakeholder approach to Internet governance by establishing a high-level advisory committee, co-chaired by former head of ICANN Fadi Chehade and Alibaba CEO Jack Ma. As its first act, the committee approved the Wuzhen Initiative, which laid out a multi-stakeholder

approach to Internet governance based on the principle of state sovereignty in cyberspace. The committee was tasked with promoting this message on the international stage and advising the Cyber Administration of China on the planning of future conferences.[29]

Since its establishment, few details about the committee's activities have been forthcoming. During the 2016 World Internet Conference (WIC), Chinese state media reported that Chehade and Jack Ma chaired a meeting of the high-level advisory committee, apparently the second time the group has met. The product of that meeting, a report on the state of the Internet, reaffirmed the principles of the Wuzhen Initiative but offered no further developments.

Despite a significant investment of time, money, and political capital, the reach and influence of the World Internet Conference remain limited to China's friends.[30] Most of the heads of government that have attended are from small states or the SCO. The United States and other Western governments have sent representatives from the embassies in Beijing, and even the tech companies, with a few exceptions, sent country heads, not CEOs or CFOs.

Cyberterrorism

Chinese diplomatic approaches to cyberterrorism originated out of norm-building efforts in the SCO. While the SCO was originally intended to demilitarize borders and build confidence among participants, its agenda expanded to economic initiatives and nontraditional security threats. In particular, the SCO focused on the "three evils": terrorism, separatism, and extremism.[31] In 2007, when the SCO began working on a code for information security, cooperative efforts moved online as members have tried to counter the use of the Internet for fund-raising, propaganda, recruitment, and organizing of attacks. The SCO's Regional Anti-Terrorist Structure coordinates cooperation among various cyber agencies in member states and maintains a database of information on suspected terrorist organizations and activities. In October 2015, China conducted its first joint Internet antiterrorism exercise, Xiamen 2015. SCO members worked on improving information sharing and cross-border coordination to respond to a simulated terrorist group's usage of social media to incite terrorist activity.[32]

In September 2014, at the UN Security Council Summit on Terrorism, Chinese Foreign Minister Wang Yi noted that "social media has become a battlefield for terrorist

and extremist groups to instigate their ideology, a tool to plot terrorist attacks and a platform to recruit terrorists."[33] Wang proposed stepped-up information sharing as well as "resolute measures" to stop the use of social media to spread extremist ideas. Internet companies in particular should exercise self-restraint, Wang said, and suggested that the United Nations should work on a code of conduct for the global technology industry.

Two months later Beijing hosted a symposium on combating cyberterrorism organized by the Global Counterterrorism Forum, an informal platform of twenty-nine countries, the EU, and various regional and UN agencies to support the implementation of the UN's Global Counter Terrorism Strategy. At the symposium, Vice Foreign Minister Zhang Yesui noted that China was also a victim of cyberterrorism as members of the East Turkistan Islamic Movement have used social media to carry out terrorist activities.[34]

The 2016 National Cyberstrategy suggests that Beijing will continue to focus antiterrorism efforts on the United Nations. Beijing will "support the United Nations to play a leading role, promote the formulation of international norms for cyberspace that are universally recognized by all sides, and an international treaty on antiterrorism in cyberspace."

Given the stark national differences on the criteria governing censorship, surveillance, and what qualifies as illegal content and separatist activity, there is little likelihood of a treaty gaining broad support. But Beijing may hope that it will make more progress in bilateral discussions. In the minds of some Chinese analysts, the growing concern over the hacking of political parties, "fake news," and interference with elections in the United States, France, Germany, Netherlands, and other countries points to some shared interests. Some Chinese participants in a US-China Track II dialogue, for example, suggested that the United States shift its international dialogue on cyber norms to include influence operations, or at the least moderate its criticism of Internet censorship and the Great Firewall.[35]

Commercial IT Diplomacy

Beijing has used trade and investment in ICT infrastructure as an economic and indirect political tool. Chinese efforts in Africa, Southeast Asia, and Central Asia are designed to access markets as well as create support for Beijing's foreign policy and cyberspace norms. Investment, however, does not always turn to influence. Private

firms are focused on profits, and even state-owned enterprises are highly motivated by economic incentives that may run counter to Beijing's goals. Moreover, different state agencies pursue different goals.

Still, there has been widespread concern that economic ties provide Beijing with direct and indirect influence and leverage. Simply by providing alternative sources of funding, Beijing can undermine US and European efforts on norms development. US and European aid often comes with conditionality in regard to democracy, transparency, and accountability. As the EU's defense and foreign policy think tank put it in a report on cyber capacity-building, "The reality is that as a donor, the EU does not operate in a vacuum and so must be prudent; recipients can go to China for funding if they feel the EU is expecting too much from them."[36]

In 2005, Huawei set up a training school in the Nigerian capital, Abuja. Five years later, Chinese telecommunications companies Huawei and ZTE were active in fifty African countries, providing communications services for more than 300 million African users. The two Chinese firms have training centers in nine African countries and built national fiber-optic communications networks and e-government networks for more than twenty countries.[37] Preferential loans and buyer credits were provided to telecoms as part of the "go out" policy to promote the internationalization of Chinese firms.[38]

Much of the current investment and trade occurs as part of the One Belt, One Road (OBOR) initiative, a development strategy focused on connectivity and cooperation in countries between China and Eurasia. OBOR has two components: the Silk Road Economic Belt, which connects China to the Persian Gulf, Mediterranean, and Indian Ocean overland; and the Twenty-first Century Maritime Silk Road, which links regional waterways. Chinese investment—approximately $51.1 billion, according to state media—has flowed into a network of railways, roads, pipelines, ports, mines, and utility grids. The largest investments are in energy and mining, infrastructure, and manufacturing sectors.[39] Official Chinese documents have also stressed the need to build an "information silk road" through cross-border optical cables and other communications trunk line networks, transcontinental submarine optical cable projects, and spatial (satellite) communication.[40] In December 2016, the Ministry of Industry and Information Technology outlined a two-year plan of building and upgrading telecom networks in Africa, with investments expected to total $173.73 billion.[41]

Chinese firms have invested in nodes along the Belt and Road. China's state-owned telecommunication companies are planning new operations in Africa and Southeast Asia. China Comservice, a subsidiary of China Telecom, announced the "Joint Construction of Africa's Information Superhighway between China and Africa" with investment amounting to $15 billion and a 150,000-kilometer optical cable covering forty-eight African countries. China Unicom is laying optical cables to connect Central Asia, Southeast Asia, Africa, and South America.[42] Private companies have also been active. In 2016, ZTE agreed to take over Turkish company Netas Telekomünikasyon for up to $101.28 million in a deal that would expand its operations across key markets covered by OBOR.[43]

Trade and investment are paralleled by an effort to influence the next generation of technology standards. After China joined the World Trade Organization, it mounted a broad effort to define technology standards in software, hardware, and communication technologies. Chinese policymakers believed that controlling a standard ensured the capture of a large share of market value. Or as a phrase popular in the technology press in China put it, third-class companies make products, second-class companies develop technology, first-class companies set standards.[44] China was especially active, although not particularly successful, in trying to define standards for third-generation cell phones (TD-SCDMA), WiFi (WAPI, or WLAN authentication and privacy infrastructure), DVDs (AVS, the audio-video coding standard), and RFID (radio frequency identification). China also increased its skill and sophistication in global standards organizations.

Beijing is focused on the next generation of Internet and communication technologies, sending large delegations to technical standards meetings. Nigel Inkster notes that China sent more than forty delegates to a 2015 meeting of the Internet Engineering Task Force, a level of engagement that "amounts to the swarming of the global-governance agenda."[45] China has been active in an International Telecommunication Union (ITU) leadership group on digital object architecture, an information management system that may play a large role in the "Internet of things."[46] According to the *Wall Street Journal,* Huawei sent twice as many representatives as did other telecoms to a 2016 meeting in Vienna to define capabilities and specifications of fifth-generation (5G) mobile.[47]

As noted above, the conversion of economic ties to political influence is often indirect. Moreover, globalizing Chinese firms have an interest in an open Internet

and transparent standards (technological and legal) that allow companies to take advantage of scale and avoid multiple competing national requirements that splinter the market. They may in the long term become norm entrepreneurs. Huawei, for example, has developed, with Microsoft and East West Institute, a "buyer's guide" for governments and corporations on acquiring more secure ICT products and services. This is an attempt to develop some global norms to ameliorate cybersecurity concerns in government procurement decisions.[48]

In the short term, at least, the presence on the ground of Chinese engineers, managers, and foreign ministry officials is likely to reinforce a natural tendency among developing countries, especially those with authoritarian governments, to embrace a vision of the Internet that puts states at the center. These countries often lack cybersecurity expertise, have a long history of dealing with the ITU, and see the multi-stakeholder process as expensive, opaque, and inefficient.

Bilateral and Regional Diplomacy

Cyber issues make up an increasingly important part of China's bilateral and regional relations. When the United States first began calling out China for cyber-enabled theft of intellectual property, Beijing's initial strategy was denial and misdirection. Each announcement that Chinese hackers were behind an attack was met with protests that hacking was illegal in China and that China was the biggest victim in cyberspace. Bilateral cybersecurity discussions were clearly something Washington wanted more than Beijing. While the United States wanted to engage broadly with the 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,* 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.[49]

Beijing seemed content to follow this strategy until Washington began ramping up the direct pressure. In March 2013, National Security Adviser Tom Donilon gave a speech that spoke of the "serious concerns about sophisticated, targeted theft of confidential business information and proprietary technologies through cyber-intrusions emanating from China on an unprecedented scale."[50] In June 2013, during their meeting in California, President Obama reportedly warned President Xi that cyberespionage would seriously damage the bilateral relationship. Soon after

the summit's end, however, Snowden appeared in Hong Kong. The disclosures of widespread NSA operations allowed Beijing to deflect and criticize the United States. US efforts on economic cyberespionage stalled.

China suspended all bilateral discussions after the indictment of five PLA hackers in May 2014. Beijing used a Track II dialogue between the Center for Strategic and International Studies and the China Institute of Contemporary International Relations for annual updates on the cybersecurity situation, but suggested that the official dialogue would only resume after the indictments were lifted. This impasse ended in part because Washington threatened sanctions on China just weeks before Xi was to arrive at the White House for his first state visit in September 2015.

The agreement that was signed has served as a template for managing cyber relations with Britain, Germany, and other Western states. In part to avoid the sanctions, and in part because of domestic considerations, Beijing and Washington agreed not to "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."[51] Both sides also agreed to identify and endorse norms of behavior in cyberspace and to establish two high-level working groups (one on security, one on crime) and a hotline for crisis response.

The group on security issues met only once before the end of the Obama administration, but the cybercrime group reported some small progress. The two sides established a point of contact and a designated e-mail address and successfully cooperated on taking down some botnets and fake websites.[52] After President Trump met President Xi in Florida in April 2017, Washington and Beijing agreed to a United States-China Comprehensive Dialogue that will have four pillars, including one on law enforcement and cybersecurity.[53]

With the United Kingdom, China has held an annual high-level security dialogue that also primarily focuses on cybercrime. In 2016, for example, Beijing and London agreed to "respond promptly to any request for information or assistance from the other participant in relation to malicious activities." They also stated that they would strengthen cooperation on preventing the use of the Internet to incite, recruit, finance, and plan terrorist activities.[54] Starting in 2012, an EU-China Cyber Taskforce began meeting during the annual EU-China summit, and has met five times since.[55] The task force appears to be a forum for the EU to express concerns about domestic Chinese

cybersecurity policies as well as discussions about Internet governance and the roles of government in cyberspace.

In addition to the United States, Beijing's most important bilateral relationship is with Moscow. The two sides signed an agreement on cooperation in the field of international information security in 2015.[56] Like the 2011 and 2015 codes of conduct, the agreement defines information security broadly to include transmission of information that threatens political and social systems. It also embraces a "multilateral, democratic and transparent management system" for the Internet, giving states a greater role in the governance process. Unlike the previous efforts, the agreement contains a list of concrete measures including the creation of contact points and communication channels and joint scientific projects. These projects are to be coordinated and evaluated through two consultation meetings a year. Moreover, both countries agreed to cooperate in the creation and dissemination of international legal norms in cyberspace and to coordinate their positions in various international forums, including the United Nations.[57]

The most widely reported provision of the agreement was a "nonaggression" pledge whereby Russia and China agreed to refrain from "computer attacks" against each other. The phrasing was vague and does not seem to cover, or at least prevent, espionage. In February 2017, for example, Qihoo 360 released its annual report on advanced persistent threats (APTs) active in China, naming thirty-six groups spying on China, including APT 28, which has been associated with Russian intelligence. (FireEye noted that Chinese actors tried to compromise Russian defense contractors and engineering firms in the energy sector.[58])

The most consequential part of the agreement regards cooperation on the development of the next generation of Internet filtering technologies. Fang Bingxing, credited with being the father of the Great Firewall, and Lu Wei, head of the Cyberspace Administration of China, went to Moscow in April 2016 for the Russia-China ICT Development & Security Forum to promote the Chinese version of Internet control. In June, Russian President Vladimir Putin went to Beijing and signed a joint communique about cyberspace.[59]

China may also provide some of the hardware needed to store data under Yarovoya's Law. The law requires Internet service providers, cell phone operators, and search engines and other web services to store all Russian traffic, including all private

chat rooms, e-mails, and social network posts, for as long as six months at their own expense as of July 1, 2018. Metadata is to be stored for three years. Some have estimated that the storage requirements for the law—more than 59 million terabytes of data—might cost close to 2.5 trillion rubles ($39 billion). Huawei reportedly held talks with Bulat, the Russian telecomm equipment manufacturer, to provide hardware.[60]

Beijing also uses cyber issues to reinforce its regional position and to bolster its leadership role in regional and developing country groupings. The International Strategy, for example, notes China's participation in China-Japan-Korea cyber policy consultation, ARF and Boao Forum for Asia, as well as the Forum on China-Africa Cooperation (FOCAC), China-Arab States Cooperation Forum, Forum of China and the Community of Latin American and Caribbean States, and the Asian-African Legal Consultative Organization.

Conclusion

Beijing has, in a relatively short span, developed and implemented a broad cyber diplomacy. Many of the ideas and practices that make up China's cyber statecraft existed previously. But bringing them all together in a set of public statements and organizations is an important step, acting as a signpost to Chinese officials working across a range of issues and providing some degree of predictability to Beijing's partners. In effect, Chinese officials have moved from a reactive position to a much more assertive effort to shape cyberspace.

Measured against its objectives—limiting the threat to regime legitimacy, extending Beijing's influence, and countering US advantages—China's diplomacy would appear relatively successful. While not solely the result of Chinese efforts, the idea that cyberspace is a sovereign space like any other is now widely accepted. Efforts to operationalize this idea, however, have gained more traction and support from like-minded countries, especially developing states worried about domestic stability, than with the more advanced economies.

The greatest uncertainty for Beijing moving forward is the state of US-China relations. The 2011 White House International Cyber Security Strategy's advancement of a "global, open, interoperable, and secure" Internet was nested within a larger trade and military framework. If, under the Trump administration, the United States is less willing to shoulder the burden of maintaining an open trade system, it can be expected that efforts in cyberspace will be replaced with a more bilateral, transactional

approach. Other countries will fill the vacuum and write new economic and political rules. Beijing is likely to promote its vision of Internet sovereignty and to adopt a selective globalization, furthering regional agreements that serve its own interests and exclude the United States and Europe.

Washington is also far less likely to censure Beijing's censorship and filtering of the Internet. Given that the Trump administration has so far prioritized fighting extremists over criticizing the domestic policies of countries such as Egypt and Bahrain, China may have reason to think that pragmatism will also guide US-China policy in cyberspace. The end of the "Internet freedom agenda" will not only remove a great source of irritation for China, but could also lead it to believe that it will find some common space with the United States, perhaps on fighting terrorist uses of the Internet. In the past, cooperation has been limited by US concerns about agreeing to China's identification of some Uighur and Tibetan groups as terrorists and on restrictions of free speech, but Beijing will continue to raise the issue and may find a more welcome reception in the new White House.

These are the possibilities for greater cooperation, but the relationship could also become increasingly contentious. As of April 2017, the agreement signed by President Obama and President Xi to crack down on cyber commercial espionage appears to be holding. A report by FireEye found a significant downturn in activity, a finding that has been supported in several public statements from US officials, though the attacks could be stealthier and more focused.[61] A significant rise in activity, however, could easily push cybersecurity back to the top of the US-China agenda and lead to more pressure from Washington.

The first summit between Xi and Obama produced more continuity in the bilateral relationship than was expected. However, increased cyber activity would be a relatively low cost method for Beijing to signal its displeasure if the Trump administration were to pursue tariffs or other punitive trade sanctions; if tensions were to rise in the South China Sea or Taiwan Strait; or if the two sides widely disagreed over how to address the worsening security situation on the Korean peninsula. Chinese hackers, for example, reportedly targeted South Korean entities involved in deploying the Terminal High Altitude Area Defense missile system.[62]

The most likely outcome in the near term is that cybersecurity issues remain an important issue in the bilateral agenda, but fairly low down the list. Dropping

the Internet freedom agenda will reduce some of the heat in cyberspace issues, but will not open many new avenues for cooperation. China will continue to push its diplomatic agenda on cyber sovereignty, but is likely to make the most progress on shaping cyberspace through OBOR and other commercial tools.

NOTES

1 Nigel Inkster, "China's Cyber Power," *Adelphi Series,* no. 456, May 23, 2016.

2 "National Cyberspace Security Strategy," *China Copyright and Media,* December 27, 2016, https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy/.

3 Andrew Keane Woods, "The Tallinn Manual 2.0, Sovereignty 1.0," *Lawfare* (blog), February 8, 2017, https://www.lawfareblog.com/tallinn-manual-20-sovereignty-10.

4 Office of the Press Secretary, White House, "Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," May 11, 2017, https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal.

5 Peter Baker, "For Trump, a Focus on U.S. Interests and a Disdain for Moralizing," *New York Times,* April 4, 2017, https://www.nytimes.com/2017/04/04/us/politics/syria-bashar-al-assad-trump.html.

6 Hannah Beech, "Rex Tillerson's Deferential Visit to China," *New Yorker,* March 21, 2017, www.newyorker.com/news/news-desk/rex-tillersons-deferential-visit-to-china.

7 Paul Rosenzweig, "Revised Draft Trump EO on Cybersecurity," *Lawfare* (blog), February 9, 2017, https://www.lawfareblog.com/revised-draft-trump-eo-cybersecurity.

8 State Council Information Office, People's Republic of China, "International Strategy of Cooperation on Cyberspace," March 2, 2017, www.scio.gov.cn/32618/Document/1543874/1543874.htm.

9 State Council Information Office, People's Republic of China, "The Internet in China," *Xinhua,* June 8, 2010, http://news.xinhuanet.com/english2010/china/2010-06/08/c_13339232.htm.

10 Chen Yiming, "US Covertly Building 'Shadow Internet,' " *People's Daily,* June 15, 2011; Yang Ziyan, " 'Cut Off the Internet' to Challenge Internet Control Power," *People's Daily* (overseas edition), August 9, 2012. Both quoted in Michael Swaine, "Chinese Views on Cybersecurity in Foreign Relations," *China Leadership Monitor* no. 42 (Fall 2013), www.hoover.org/sites/default/files/uploads/documents/CLM42MS.pdf.

11 Lu Chuanying, "The International Cyberspace Rule-based System and the China-U.S. New Type of Great Power Relations," *People's Daily—Theory Channel,* December 2, 2016, http://theory.people.com.cn/n1/2016/1202/c386965-28920732.html.

12 Milton Mueller, *Network and States: The Global Politics of Internet Governance* (Cambridge, MA: MIT Press, 2010).

13 Hillary Clinton, "Remarks on Internet Freedom" (speech), The Newseum, Washington, DC, January 21, 2010, https://2009-2017.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm.

14 "Big Points Buried in the U.S. Cyberwar Strategy," *Xinhua,* April 7, 2015, http://news.xinhuanet.com/zgjx/2015-04/07/c_134128303.htm.

15 "International Code of Conduct for Information Security," United Nations General Assembly, September 14, 2011, www.rusemb.org.uk/data/doc/internationalcodeeng.pdf.

16 NATO Cooperative Cyber Defence Centre of Excellence, "An Updated Draft of the Code of Conduct Distributed in the United Nations—What's New?" February 10, 2015, https://ccdcoe.org/updated-draft-code-conduct-distributed-united-nations-whats-new.html.

17 Sarah McKune, "An Analysis of the International Code of Conduct for Information Security," *The Citizen Lab,* September 28, 2015, https://citizenlab.org/2015/09/international-code-of-conduct/.

18 "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, June 24, 2013, www.un.org/ga/search/view_doc.asp?symbol=A/68/98&referer=/english/&Lang=E.

19 Adam Segal, "Cyberspace Cannot Live without Sovereignty, Says Lu Wei," *Asia Unbound* (blog), Council on Foreign Relations, December 10, 2013, http://blogs.cfr.org/asia/2013/12/10/cyberspace-cannot-live-without-sovereignty-says-lu-wei/.

20 United Nations, "Developments in the Field of Information and Telecommunications in the Context of International Security," July 22, 2015, http://undocs.org/A/70/172.

21 Joseph Marks, "U.N. body Agrees to U.S. Norms in Cyberspace," *Politico,* July 9, 2015, www.politico.com/story/2015/07/un-body-agrees-to-us-norms-in-cyberspace-119900.

22 Scott Warren Harold, Martin C. Libicki, and Astrid Stuth Cevallos, "Getting to Yes with China in Cyberspace," Rand Corporation, 2016, https://www.rand.org/pubs/research_reports/RR1335.html.

23 Craig Timberg and Ellen Nakashima, "Chinese Hackers Suspected in Attack on The Post's computers," *Washington Post,* February 1, 2013, https://www.washingtonpost.com/business/technology/chinese-hackers-suspected-in-attack-on-the-posts-computers/2013/02/01/d5a44fde-6cb1-11e2-bd36-c0fe61a205f6_story.html.

24 State Council Information Office, "International Strategy of Cooperation on Cyberspace," March 2, 2017, www.scio.gov.cn/32618/Document/1543874/1543874.htm.

25 Joseph Marks, "New International Cyber Rules Likely Off the Table for UN Experts Group," *Nextgov,* February 6, 2017, www.nextgov.com/cybersecurity/2017/02/new-international-cyber-rules-likely-table-un-experts-group/135193/.

26 David Bandurski, "Envisioning the Splinternet," *China Media Project,* November 20, 2014, http://cmp.hku.hk/2014/11/20/chinas-splinternet-making-insularity-global/.

27 Josh Chin, "I Don't Declare: China's Struggle to Sell Vision at Internet Summit," *Wall Street Journal,* December 9, 2015, https://blogs.wsj.com/chinarealtime/2015/12/09/i-dont-declare-chinas-struggle-to-sell-vision-at-Internet-summit/.

28 "Remarks by H. E. Xi Jinping, President of the People's Republic of China, at the Opening Ceremony of the Second World Internet Conference," Ministry of Foreign Affairs, People's Republic of China, December 16, 2015, www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t1327570.shtml.

29 Kieren McCarthy, "The Firewall Awakens: ICANN's Exiting CEO Takes Internet Governance to the Dark Side," *The Register,* December 18, 2015, https://www.theregister.co.uk/2015/12/18/ex_icann_ceo_will_work_with_china/.

30 Adam Segal, "China's Internet Conference: Xi Jinping's Message to Washington," *Net Politics* (blog), Council on Foreign Relations, December 16, 2015, https://www.cfr.org/blog-post/chinas-internet-conference-xi-jinpings-message-washington.

31 Nargis Hamroboyeva, "SCO Member Nations to Tighten Fight Against Cyber Terrorism," *Asia-Plus,* April 9, 2012, http://news.tj/en/news/sco-member-nations-tighten-fight-against-cyber-terrorism.

32 Peter Wood, "China Conducts Anti-Terror Cyber Operations with SCO Partners," *China Brief* 15, no. 20, Jamestown Foundation, October 19, 2015, https://jamestown.org/program/china-conducts-anti-terror-cyber-operations-with-sco-partners/.

33 Wang Yi, "Working Together to Address the New Threat of Terrorism" (speech), Ministry of Foreign Affairs, People's Republic of China, September 24, 2014, www.fmprc.gov.cn/mfa_eng/zxxx_662805/t1195235.shtml.

34 "Symposium on Combating Cyber-Terrorism of Global Counterterrorism Forum," Beijing, Ministry of Foreign Affairs, People's Republic of China, November 18, 2014, www.fmprc.gov.cn/mfa_eng/wjbxw/t1212941.shtml.

35 Adam Segal, "The Continued Importance of the U.S.-China Cyber Dialogue," *Net Politics* (blog), January 23, 2017, https://www.cfr.org/blog-post/continued-importance-us-china-cyber-dialogue.

36 "Capacity Building in Cyberspace: Taking Stock," report from seminar organized by the European Union Institute for Security Studies, Brussels, November 19, 2013, www.iss.europa.eu/uploads/media/EUISS_Cyber_Task_Force_Report.pdf.

37 Andrea Marshall, "China's Mighty Telecom Footprint in Africa," *New Security Learning,* February, 14, 2011, www.newsecuritylearning.com/index.php/archive/75-chinas-mighty-telecom-footprint-in-africa; Daouda Cissé, " 'Going global' in Growth Markets—Chinese Investments in Telecommunications in Africa," Centre for Chinese Studies at Stellenbosch University, South Africa, April 2012, http://www.ccs.org.za/wp-content/uploads/2012/04/Telecom_Policy-Briefing_final.pdf.

38 "China's Telecommunications Footprint in Africa," Institute of Developing Economies, Japan External Trade Organization, October 2009, www.ide.go.jp/English/Data/Africa_file/Manualreport/cia_09.html.

39 Yang Yuntao, "The First Authoritative Report on 'Belt and Road' Three-year Progress Released," *China Daily,* September 26, 2016, www.chinadaily.com.cn/opinion/2016-09/26/content_26901304_2.htm.

40 "Vision and Actions on Jointly Building Silk Road Economic Belt and 21st-Century Maritime Silk Road," Consulate-General of the PRC in Vancouver, April 4, 2015, http://vancouver.china-consulate.org/eng/topic/obor/.

41 "Chinese Firm Hopes to Wire Continent with Same Strategy that Boosted Internet Access Across China," *Global Times,* March 13, 2017, www.globaltimes.cn/content/1037500.shtml.

42 "Key Connectivity Improvements along the Belt and Road in Telecommunications & Aviation Sectors," *China Go Abroad,* no. 4, EY, September 2016, www.ey.com/Publication/vwLUAssets/ey-china-go-abroad-4th-issue-2016-en/$FILE/ey-china-go-abroad-4th-issue-2016-en.pdf.

43 Bien Perez, "China's ZTE Takes Over Netas for $101m, Eyes Expansion in Turkey," *South China Morning Post,* December 6, 2016, www.scmp.com/tech/china-tech/article/2052271/chinas-zte-takes-over-netas-101m-eyes-expansion-turkey.

44 Adam Segal, *Advantage: How American Innovation Can Overcome the Asian Challenge* (New York: WW Norton, 2011).

45 Inkster, "China's Cyber Power."

46 Robert M. McDowell and Gordon M. Goldstein, "The Authoritarian Internet Power Grab," *Wall Street Journal,* October 25, 2016, www.wsj.com/articles/the-authoritarian-Internet-power-grab-1477436573.

47 Matthias Verbergt, "China's Huawei Battles to Own the Next Generation of Wireless Technology," *Wall Street Journal,* February 26, 2017, https://www.wsj.com/articles/chinas-huawei-battles-to-own-the-next-generation-of-wireless-technology-1488114002.

48 Juro Osawa, "Microsoft, Huawei Join in Cybersecurity Message," *Wall Street Journal,* September 13, 2016, https://www.wsj.com/articles/microsoft-huawei-join-in-cybersecurity-message-1473757469.

49 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.

50 Liz Flora, "Complete Transcript: Thomas Donilon at Asia Society New York," Asia Society, March 11, 2013, http://asiasociety.org/new-york/complete-transcript-thomas-donilon-asia-society-new-york.

51 "Remarks by President Obama and President Xi of the People's Republic of China in Joint Press Conference," Office of the Press Secretary, White House, September 25, 2015, https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/remarks-president-obama-and-president-xi-peoples-republic-china-joint.

52 Josh Chin, "Inside the Slow Workings of the U.S.-China Cybersecurity Agreement," *Wall Street Journal,* June 15, 2016, https://blogs.wsj.com/chinarealtime/2016/06/15/inside-the-slow-workings-of-the-u-s-china-cybersecurity-agreement/.

53 "Statement from the Press Secretary on the United States-China Visit," Office of the Press Secretary, White House, April 7, 2017, https://www.whitehouse.gov/the-press-office/2017/04/07/statement-press-secretary-united-states-china-visit.

54 "China-UK High Level Security Dialogue: Communique," GOV.UK, June 13, 2016, https://www.gov.uk/government/publications/china-uk-high-level-security-dialogue-official-statement/china-uk-high-level-security-dialogue-communique.

55 Patryk Pawlak, "Cyber Diplomacy: EU Dialogue with Third Countries," European Parliament Think Tank, June 29, 2015, www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2015)564374.

56 Andrew Roth, "Russia and China Sign Cooperation Pacts," *New York Times,* May 8, 2015, https://www.nytimes.com/2015/05/09/world/europe/russia-and-china-sign-cooperation-pacts.html?_r=0.

57 Elaine Korzak, "The Next Level for Russia-China Cyberspace Cooperation?" *Net Politics* (blog), August 20, 2015, https://www.cfr.org/blog/next-level-russia-china-cyberspace-cooperation.

58 Adam Segal, "A Fancy Bear Finds Its Way into the Middle Kingdom," *Net Politics,* Council on Foreign Relations, February 15, 2017, https://www.cfr.org/article/fancy-bear-finds-its-way-middle-kingdom.

59 Samuel Wade, "Chinese Cyberchiefs Preach Net Sovereignty in Moscow," *China Digital Times,* April 27, 2016, http://chinadigitaltimes.net/2016/04/chinese-cyberchiefs-preach-Internet-sovereignty-moscow/.

60 Mikhail Klementiev, "Russia in Talks with China's Huawei on Data Storage Technologies' Licensing," *Sputnik News,* August 24, 2016, https://sputniknews.com/science/201608241044578435-russia-huawei-bulat-data/.

61 David E. Sanger, "Chinese Curb Cyberattacks on U.S. Interests, Report Finds," *New York Times,* June 20, 2016, https://www.nytimes.com/2016/06/21/us/politics/china-us-cyber-spying.html; Joe Uchill, "Obama Administration Confirms Drop in Chinese Cyber Attacks," *The Hill,* June 28, 2016, http://thehill.com/policy/cybersecurity/285153-obama-administration-confirms-drop-in-chinese-cyber-attacks.

62 Jonathan Cheng and Josh Chin, "China Hacked South Korea Over Missile Defense, U.S. Firm Says," *Wall Street Journal,* April 21, 2017, https://www.wsj.com/articles/chinas-secret-weapon-in-south-korea-missile-fight-hackers-1492766403.

The preferred citation for this publication is 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), available at http://lawfareblog.com/chinese-cyber-diplomacy-new-era-uncertainty.

About the Author

ADAM SEGAL

Adam Segal is the Ira A. Lipman Chair in Emerging Technologies and National Security, and Director, Digital and Cyberspace Policy. An expert on cyber security and Chinese domestic and foreign policy, his most recent book is *The Hacked World Order* (PublicAffairs, 2016).

Author Photo

http://www.cfr.org/content/bios/SegalPhotoBig_1.png
credit: David White

Jean Perkins Foundation 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 cyber security, the rise of drones and autonomous weapons systems, and the need for—and dangers of—state surveillance. The working group's output, which includes the Aegis Paper Series, is also published on the *Lawfare* blog channel, "Aegis: Security Policy in Depth," in partnership with the Hoover Institution.

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