Winter 2-11-2021

Chinese Technology Platforms Operating in the United States: Assessing the Threat (Originally Published as a Joint Report of the National Security, Technology, and Law Working Group at the Hoover Institution at Stanford University and the Tech, Law & Security Program at American University Washington College of Law)

Gary Corn

Jennifer Daskal

Jack Goldsmith

Chris Inglis

Paul Rosenzweig

See next page for additional authors

Authors

Gary Corn, Jennifer Daskal, Jack Goldsmith, Chris Inglis, Paul Rosenzweig, Samm Sacks, Bruce Schneier, Alex Stamos, and Vincent Stewart

JOINT REPORT OF THE NATIONAL SECURITY, TECHNOLOGY, AND LAW WORKING GROUP AT THE HOOVER INSTITUTION AT STANFORD UNIVERSITY AND THE TECH, LAW & SECURITY PROGRAM AT AMERICAN UNIVERSITY WASHINGTON COLLEGE OF LAW

Chinese Technology Platforms Operating in the United States

ASSESSING THE THREAT

GARY CORN, JENNIFER DASKAL, JACK GOLDSMITH, CHRIS INGLIS, PAUL ROSENZWEIG, SAMM SACKS, BRUCE SCHNEIER, ALEX STAMOS, AND VINCENT STEWART

Introduction

In the fall of 2020, the Trump administration issued dual executive orders designed to effectively ban TikTok and WeChat from operating in the United States, at least in their current forms. In January 2021 it did the same with respect to Alipay and seven other Chinese-owned apps. These actions came against the background of years of executive orders and rules aimed at limiting the reach of China-based technology firms. Each of these actions was based, in significant part, on assertions of national security. Going forward, the US government has an urgent need for smart policies and practices to respond to China's growing tech sector and the spread of China-controlled platforms. The Biden administration will have to decide what to do about TikTok and WeChat. It also will need to develop a broader US strategy for addressing the range of security risks (e.g., economic, national security, cybersecurity) and threats to civil liberties posed by the spread of China-developed and -controlled technologies.

This report seeks to contribute to these efforts by suggesting a comprehensive framework for understanding and assessing the risks posed by Chinese technology platforms in the United States. It is the product of a working group convened by the Tech, Law & Security Program at American University Washington College of Law and the National Security, Technology, and Law Working Group at the Hoover Institution at Stanford University. The signatories to this report come to this issue with different perspectives and different backgrounds. But we share a common view—one reflected in numerous reports and publicly available threat assessments—that China's power is growing, that a large part of that power is in the digital sphere, and that China can and will wield that power in ways that adversely affect our national security.[1] And we assess that it will do so in novel ways that implicate numerous interests not traditionally associated with national security, such as data privacy, freedom of speech, and economic competitiveness.

That said, we also recognize that not all such threats are equal. Actions with respect to Huawei, federal bans on the use of Chinese-manufactured drones, the executive orders

targeting TikTok and WeChat, and recently suggested prohibitions on US companies doing business with foreign-owned cloud infrastructure all assert general risk to national security as a justification.[2] But the specific threats and risks posed by each of these unique technologies vary. The collateral costs and impacts of these actions differ. And the possibilities of effective mitigation measures to minimize both the risks and the collateral consequences differ as well.

The primary goal of this report is to frame, assess, and disaggregate the various national security risks associated with one specific aspect of this threat: China's ownership and control over communication platforms and other technologies used in the United States. An effective policy must start with a targeted understanding of the nature of risks and an assessment of the impact US measures will have on national security and competitiveness. To be clear, we lack sufficient information—and do not attempt—to accurately quantify the seriousness of the specific risks. Rather, our goal here is to analyze the various threats, put them into context, and offer a framework for assessing proposed responses in ways that we hope can aid those doing the risk analysis in individual cases. Moreover, while we focus this paper on communications platforms, we hope and expect the analysis to be useful in other areas.

The Strategic Landscape and Broader State of Play

To set the scene for the discussion, this section lays out the broader strategic landscape between the United States and China with respect to Chinese digital platforms and influence overseas.

The growing power of Chinese tech companies and the Chinese system Chinese technology firms are growing more competitive internationally. Chinese firms benefit from state subsidies and protectionist policies domestically, helping enable their global expansion. At the same time, the firms have shown real innovation and commercial prowess in ways that have also contributed to their global competitiveness. Of particular note, Chinese-owned apps integrate social media, financial, personal, and business functions in ways that are unknown in the West. This kind of integration is promoted by the Chinese government. It provides the government unprecedented access to information as well as a means to control and censor. It also is prized by consumers for the convenience offered by connected applications.

Meanwhile, the Chinese government pursues an increasingly assertive foreign policy that, among other objectives, seeks to advance an authoritarian capitalist model of governance that could threaten support for democracy, human rights, and the rule of law. The US intelligence community's 2019 *Worldwide Threat Assessment* described this as a coming ideological battle with the United States.[3] Beijing also leverages internet and emerging technologies to increase its foothold in technological systems around the world. Given the Chinese government's relationship to the Chinese technology sector, this leverage raises

concerns about China's ability to access data, engage in malicious influence operations abroad, and launch cyber-enabled attacks. These concerns apply to data stored outside of China's borders, even if held by companies incorporated in China, and to data held by foreign firms that have servers within Chinese borders.

Beijing's relationship to the Chinese technology sector is also evidenced in the government's concerning efforts to shift technical standards and internet protocol development (e.g., the pushing of a New Internet Protocol proposal) from open, multistakeholder bodies, to more state-controlled venues that would allow Beijing to promote standards that advantage Chinese firms.[4] There is also a concern that broader Chinese dominance in critical communications technologies like 5G presents both economic and national security risks to the United States.

It also is important to stress that "China" is not a monolith. There is friction within the Chinese system itself. Technology firms can push back—and they have done that in the past—against Chinese government data access requests in select cases. As a result, the Chinese government's ability to access data may not be as capacious as often depicted in United States commentary. There is also real debate within China about privacy as well as efforts to impose data collection limits on private firms. That said, President Xi Jinping's China has reportedly put an end to the earlier period of "reform and opening," reversing liberalization efforts in law and government and in some instances asserting extraordinary controls on some of China's best known e-commerce firms. And the system lacks checks and balances, oversight, and clear ways for individuals or companies to contest the Chinese government's technology and data access decisions.

Internet governance battle Rather than working with allies to build a coherent system for regulating the internet, the United States is in many respects at odds with key allies and partners around the world. This can, in part, be linked to the Trump administration's impact on diplomatic relationships. But other structural challenges—such as divergence on privacy and speech policy between the United States and the European Union—persist. As a result, in Europe and in many other parts of the world, governments and the public at times make a false equivalency between the US and Chinese internet governance systems. They sometimes point, for example, to the US system of foreign intelligence collection as a violation of their citizens' rights and interests and suggest that it is equivalent to the ways in which China gathers data and conducts surveillance.

Chinese online threat The US intelligence community assesses that China is engaged in active, ongoing cyberespionage against the United States.[5] This is underscored by numerous reports and indictments of cyber-enabled trade secret theft in recent years.[6] The intelligence community also assesses that China presents a growing threat of offensive cyber operations against our core military and critical infrastructure systems and is expanding its ability to engage in influence operations against the United States and its citizens.

National security shift Foreign intelligence collection and espionage are evolving with the growing digitization of society. Technological embeddedness and diffusion (e.g., smartphone apps, facial recognition cameras, the Internet of Things) have opened up the possibility of new and broader vectors of data collection on individuals or populations without the same kind or degree of resource limitations of the past.

There is also a risk that anyone or any device or system—irrespective of country of origin—could become a threat vector. Every piece of software or hardware has vulnerabilities that can be exploited. Every piece of software or hardware may also produce vulnerabilities in its interaction with other systems and devices. And with a globally entangled digital supply chain, compromises of one system can further expose many others to subsequent compromise, as was recently seen in the case of the SolarWinds compromise. As a result, the US homeland and its connected infrastructure on American soil are at risk in distinctly new ways, not just through vulnerabilities in devices but through greater consumer dependence on global goods as well.

Privacy and cybersecurity failures Pervasive data collection also enables a range of actors—including, potentially, a foreign adversary like the Chinese government—to access large quantities of data. This creates significant risks, as increasingly sophisticated and powerful analytics can discover highly granular information about particular individual or group attributes and behavior via analysis of this data. Among other concerns, this can be used for identity exploitation, influence, and control. The ability to collect stems from several factors including the private sector's mass data collection, weak cybersecurity practices by many companies, and the absence of effective data privacy protections in many countries around the world, notably including the United States. The lack of sufficient market incentives for private companies to invest in robust (and often basic) cybersecurity measures also harms national security with respect to data confidentiality.

Trade issues On top of all this, there is an ongoing trade battle between Washington and Beijing that is based in part on protectionist interests related to technology firms as well as a strategic goal of ensuring technological dominance on a global scale. These trade issues are increasingly intertwined with national security issues. The Trump administration's export controls on US technology going to Chinese telecom Huawei—made under the claim of national security risk but done with broad impacts on trade—are one such example.[7] Future regulation of technologies for security reasons will have broad strategic implications for global trade as well. Economic and national security risks are, as a result, becoming increasingly entangled.

Nature of Risks Associated with Data Access and Infiltration by Foreign Technology

Distinct, and often significant, national security risks are at play with respect to China's access to data and control over technologies relied on by Americans. These risks are often

grouped together in ways that blur their discrete aspects. It is thus important to specify the nature of the risks so as to ensure targeted, tailored responses that account for ripple effects on US security and prosperity and increase public confidence in the decision to respond.

Access to data The national security risks associated with access to data about national security secrets, such as core military capabilities or nuclear weapons, are widely recognized and significant. Access to data about (or technology used by) others, including those civilians who do not work in government, the defense industrial base, sensitive technology sectors, or on other parts of the critical infrastructure, creates national security risks that may not be as intuitive. Such information can be collected and aggregated, without the resource limitations of the past, in ways that create new national security risks, even if the particular topic of information collected is not, on its face, related to national security.

First, a national security threat arises if and when an individual or organization is connected with, is linked to, or becomes the person with digital keys to valued sources of information, such as critical infrastructure or governmental secrets. That individual and his or her connected systems and devices are all potential vectors for a malicious actor to gain access to sensitive data and systems (such as through email phishing to trick an individual or targeted network attacks that collect internet data in transit).

Second, as one learns more about an individual's or group's interests, thought processes, and the like, that individual or group could become a target—or potentially an asset—in an information or espionage campaign. This in turn can increase the effectiveness of both human intelligence and digital influence operations. One can, for example, imagine an influence campaign that identifies and targets American institutions with the aim of increasing the potency of Chinese messaging or undermining the willpower of US decision makers to advance US initiatives deemed contrary to the interest of the Chinese government.

Third, even if the particular individual is not a valuable source or target, his or her data can be combined with others—thus becoming a data point that subsequently enables an actor to carry out better targeting, analysis, or artificial intelligence development. The vastly expanding capabilities to combine disparate data sets and correlate information to identify individuals mean that the security risks of a particular data set are no longer confined just to the substance of the data itself. They include the data sets with which it can be combined. In that vein, as several experts have suggested, the aggregation of data in itself has potential intelligence value, even if the collection is not focused on any specific target. It enables a foreign adversary like China to glean valuable information about patterns of behavior, interests, and predispositions that could in turn be used to inform future intelligence, cyber, and information operations and, potentially, to better train artificial intelligence algorithms. That said, at some point access to additional data may have diminishing returns, such that adding more information will not add much more value for the actor.

Fourth, national security and economic risks intersect. The aggregation of immense data sets by a Chinese firm like ByteDance, for example, could help further the expansion of Chinese technology companies globally. Large data sets also drive AI technical development—and greater access therefore means greater likelihood of success, all other things being equal. These factors can further China's economic strength, intelligence exploitation, and cyber and influence campaigns.[8]

In sum, the ability of foreign actors to aggregate large volumes of data is a growing security threat, but it is important to put each case in context.

Influence operations China effectively controls its domestic information environment and has been expanding its capability to shape the information environment abroad. Chinese technology platforms potentially provide ways in which access to communications systems becomes an easy means to manipulate users. Thus far, Beijing primarily conducts influence operations to gather strategic intelligence about US policies and personnel, to acquire technology from industrial espionage targets, and to influence and shape the public narrative overseas related to Chinese domestic issues such as Hong Kong's autonomy and human rights abuses in Xinjiang.[9] In the future, it is possible that Chinese influence operations could target democratic institutions or sow panic in moments of crisis as well, further implicating national security. Already, Beijing has used influence operations during the COVID-19 pandemic to spread disinformation about the virus.

Attack vectors China could leverage access to networks and individual devices such as smartphones to conduct malicious cyber operations. Intrusions into digital infrastructure or preexisting footholds in that infrastructure (e.g., concerns about Huawei 5G) could enable China to gather information; disrupt the speed, reliability, or other functionality of systems and devices; or cause physical damage through those systems. This kind of sabotage can be uniquely damaging but difficult to detect. Poor security practices in technological standards and protocols—weaknesses in the communication rules used by different systems and devices—exacerbate these risks.

Case-Based Analysis for Individual Cases: Necessity and Proportionality

The US government needs a framework for deciding whether, in what circumstances, and how to take action with respect to Chinese-manufactured, -owned, or -controlled communications technology and systems that may pose security risks to the United States. The diffuseness, indirectness, and interconnectedness of digital threats make this consideration of collateral consequences all the more important.

Once all data collection is defined as a national security threat, then just about everything in the digital realm is a national security threat. The challenge is figuring out the risk posed in different contexts (including a nuanced assessment of the kind of collection one

is concerned about, by whom, and why it poses a threat), the tolerance for those risks, and available mitigation measures. This challenge requires a consistent and principled balancing approach to vetting and assessing risk posed by collection activities as well as the costs incurred by planned responses to such activities. It involves assessing the nature and weight to be accorded to the particular threat and subsequently balancing the mitigation of said threat against the nature and weight of a chosen response's potential collateral consequences.

A necessity and proportionality framework helps with this analysis. This framework involves balancing the need to act against the various costs of doing so. It helps decision makers analyze whether and in what circumstances mitigation measures can help alleviate the national security risks identified. Several components and variables are involved in identifying whether a particular technology presents a national security risk. It is not within the scope of this effort or within the capability of this group to make those determinations with respect to any particular technology or platform with any reasonably certain degree of accuracy. This report instead offers a framework for evaluating such risk.

1. Proper Identification of Risk

Step one is to accurately frame the threat's nature, its directness, the degree to which it is likely to manifest, and its relative immediacy, among other factors. The risks posed by threats directed against core military or other traditional national security concerns are obvious. The risk, however, diminishes where the threat is based on general data collection considerations, which are more uncertain and diffuse. These general data collection concerns are of two distinct varieties: concerns about the collection of data regarding the operation (and perhaps vulnerability) of critical infrastructure systems; and similar concerns about broader collection related to consumers and their behavior. When talking about the threat posed by access to data from communications platforms and apps, it is also critical to assess whether and to what extent the data provides additional value beyond what is available to China via scraping of publicly available data sources, purchasing from data brokers, illegal theft, or other alternative mechanisms of acquiring the data.

2. Assessment of Collateral Consequences

Step two is to delineate and assess collateral consequences. Risk mitigation measures should be proportionate to the assessed need to act. Within this framework, the proportionality analysis should take into account the potential collateral consequences to the United States, its partners, its allies, and its citizens. Such policies should also include clear red lines for determining when the negative collateral impacts are deemed disproportionate to the need or otherwise unacceptable. The United States should at all times be wary of actions that give authoritarian regimes rhetorical ammunition to defend their own policies and establish dangerous precedents for other countries to do the same.

Depending on the technology or platform at issue, these collateral concerns might include, but are not limited to, negative impacts on:

Individual rights Information controls on internet traffic or internet companies could stifle speech and association in ways that undercut individual rights, as demonstrated by a court ruling that found the Trump administration's WeChat "ban" violated the First Amendment.[10] Such controls also could undermine important freedoms that do not receive First Amendment protection. Regulation could also collaterally impact individuals' ability to associate, organize, and assemble in the modern age. The WeChat executive order was a similar manifestation of this problem, as it would, if put into effect, have blocked many American users from interacting with friends, family, and business partners located in China. More generally, it is critical that US mitigation measures should account for America's values and commitments, including its commitment to diversity as a nation of immigrants.

Economic competitiveness and innovation Much of the world looks to the United States as a global leader on technology policy. Yet US technology is also, for many, something to be feared, or at least critiqued. There is, as a result, a significant risk that US bans based on foreign ownership will come back to haunt American companies. Already, many countries are levying restrictions on their digital markets and raising digital trade barriers to foreign firms. American businesses will suffer if it becomes an increasingly common, accepted practice to kick out apps and other services based on the fact that they are foreign-owned. Restricting transactions between US and Chinese companies may also lead to American companies getting shut out of markets where those Chinese companies operate, thereby ceding ground to Chinese or other companies to provide those services instead.

Meanwhile, severing or modulating rich, free-flowing connectivity among diverse pools of perspective, talent, and research will almost certainly create headwinds to innovation. This will affect productivity, thereby reducing the size of the economic pie, apart from how shares within that pie are divvied up.

Security Some mitigation measures will likely drive individual users to alternative social media and communications platforms. Proposed mitigation measures should take into account the potential for damaging the US government's ability to access communications for legitimate intelligence purposes. For similar reasons, there may be a benefit in encouraging, rather than discouraging (or prohibiting), such entities from using US-based cloud providers.

3. Assessment of Mitigation Measures

Finally, step three is to assess measures that might mitigate the risks identified. Possible measures include:

Restricting access Key considerations include the following: where the data is stored, how the data is stored (e.g, is it encrypted?), where and how the data is transmitted, who within the company can access it, who from any third-party suppliers or subcontractors can access it, and whether the adversary government has any formal or informal access. These also include technological considerations as well as logistical and ownership questions (e.g., who provides cloud storage and what rules is that provider bound by?).

Audits and reviews Effective audits and reviews can minimize and identify national security risks. The United Kingdom has instituted (and has recently planned to expand) a testing and evaluation center for 5G telecommunications equipment that probes for security vulnerabilities and assesses security risk. The Cyberspace Solarium Commission's supply chain report recommends better product testing in the United States to promote stronger security across the broader digital supply chain.[11] Audits and reviews should be similarly imposed on particular entities and technologies that carry national security risks.

Broad Policy Responses

In addition to creating a proportionality framework to identify and respond to particular risks, the United States needs to adopt a range of broad policy responses to strengthen its defenses, support our economy, minimize the risk that might otherwise be posed by any particular actor or entity, and build alliances that promote a safe and secure internet while protecting core values. These broad policy responses are a key part of the solution. They shift the backdrop against which individual cases are assessed.

Stronger cybersecurity Improving overall cybersecurity defenses across all sectors of society would help provide needed protection against the aforementioned threats as well (of course) as many others. Stronger cybersecurity protections at home would introduce barriers and friction to China's ability to exploit the cyber environment to its strategic advantage. Securing digital systems and infrastructure would have broader benefits as well, helping to protect against an array of different threats. The SolarWinds incident is just the latest demonstration of the importance of bolstering security in a globally interconnected digital supply chain.

Other elements of strong cybersecurity include the development of better means to track, detect, and proactively defend particular systems of interest—something that is largely a human-based endeavor, albeit aided by technology. In addition, there is a need to leverage coalitions (e.g., international, private-public) across the connected fabric of cyberspace so that China is required to defeat a coalition rather than picking off one unlucky victim at a time.

Privacy legislation Placing better controls on data collection, sale, and aggregation by private companies would help ensure better data security. In turn, this would limit the amount and type of data that foreign actors can exploit and the potential for malicious actors (including foreign adversaries such as China) to engage in such activities as espionage and disinformation campaigns. In particular, strong privacy legislation should include limitations on data collection by private companies as well as limits on the data brokerage industry, so as to restrict its buying and selling of information.

Clear risk-based framework for foreign apps As part of any policy on the security of all software, the US government needs to be explicit about the alleged security risks posed by foreign software and the requirements for addressing those risks. Clear criteria as to when a foreign app poses a national security risk will help ensure consistency and stability of enforcement.[12] This should not mimic Beijing's approach to "cyber sovereignty" but should put in place an approach that establishes strong, generally applicable safeguards while enabling data flows that meet those standards.

Policies for global cloud computing The United States should demand appropriate privacy and security controls—such as those put forward by both the National Institute of Standards and Technology (NIST) and the International Organization for Standardization (ISO)—on cloud security standards.[13] These standards help ensure the safe routing of data between different locations around the world.

International engagement These challenges will not be solved purely through domestic means. Three prongs of international engagement are vital to US success on these issues.

First, alliances: the United States should partner with key allies in the democratic world to advance norms, standards, policies, and principles that support better cybersecurity, better privacy, and preservation of a free, open, and secure internet. This should include a particular focus on US-EU engagement.[14] In addition, the United States should pursue alliances with those within China's geographic and influence orbit, including Japan, South Korea, Singapore, India, and Australia.

Second, vision: the United States needs a stronger vision of internet governance that places management of harm front and center, while also safeguarding core freedoms and resisting authoritarian systems of surveillance and control.

And third, standards: a defining feature of Beijing's approach to internet governance is pursuing the replacement of open and interoperable internet standards with standards designed to promote Chinese technology and a Chinese interpretation of economic and national security. The US government has largely remained on the sidelines in this contest (although US technology companies remain actively engaged) because of its historically

hands-off approach to the internet and desire to not mimic Beijing's state-heavy approach to technology standards. It is time for Washington to carefully consider a renewed form of engagement with standards bodies.

Investment in US industry Finally, the US government should invest intelligently in American industry. The Cyberspace Solarium Commission, for instance, recommended in its full report that the US government invest more in promoting cyber resilience to shift market incentives.[15] And its supply chain white paper recommended targeted infrastructure investment to boost US competitiveness.[16] These are valuable starting points.

Conclusion

The US response to the growing threat posed by China-controlled internet platforms lacks coherence. The United States needs a clear, effective, and consistent strategy on these issues. Such a strategy requires a clear-eyed view of the interconnected threats to our economy, national security, and civil liberties posed by China; a comprehensive assessment of the costs and benefits of proposed responses; and the building of structures, coalitions, and international alliances that collectively resist authoritarian systems of control. This paper seeks to contribute to that effort by providing a framework for assessing and evaluating risk.

ACKNOWLEDGMENTS

The signatories wish to express their deep gratitude for the assistance provided by the Technology, Law & Security Program's senior researcher, Jenna Ruddock, and research fellow Justin Sherman; Harvard Law School student Casey Corcoran; and the many experts who graciously shared their time and expertise to inform this report.

NOTES

1 We focus in this report on China because the combination of economic influence and national security threat posed by China is categorically different from that posed by other nations. We see, for example, the threat to national security posed by the Russian SolarWinds intrusion as of an extremely grave, but different, nature. More specifically, our focus is on the security threats posed by Chinese state organs and their relationship to Chinese-owned or -controlled technology manufacturers, developers, and providers. As noted below, measures adopted to mitigate these risks should account for and be consistent with the United States' commitment to individual rights and core freedoms.

2 Chaim Gartenberg and Russell Brandom, *US Government Adds DJI to Commerce Blacklist over Ties to Chinese Government*, The Verge (Dec. 18, 2020), https://www.theverge.com/2020/12/18/22188789/dji-ban-commerce-entity-list-drone-china-transaction-blocked; Ashley Gold, *Scoop: Trump Admin Mulls Blocking Cloud Firms from Countries like China*, Axios (Dec. 4, 2020), https://www.axios.com/scoop-commerce-mulls-blocking-cloud-firms-from-countries-like-china-95e000d7-c6d2-4513-b208-2f5a158f1b58.html; Bureau of Industry and Security, *Huawei Entity List Frequently Asked Questions (FAQs)* (Dec. 3, 2020), https://www.bis.doc.gov/index.php/documents/pdfs/2447-huawei-entity-listing-faqs/file; Exec. Order No. 13,492, 85 Fed. Reg. 48637 (Aug. 11, 2020), https://www.federalregister.gov/documents/2020/08/11/2020-17699/addressing-the-threat-posed-by-tiktok-and-taking-additional-steps-to-address-the-national-emergency; Exec. Order No. 13,943, 85 Fed. Reg. 48641 (Aug. 11, 2020), https://www.federalregister.gov/documents/2020/08/11/2020-17700/addressing-the-threat-posed-by-wechat-and-taking-additional-steps-to-address-the-national-emergency.

3 Office of the Dir. of Nat'l Intelligence, *Worldwide Threat Assessment of the US Intelligence Community* (Jan. 29, 2019), https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf [hereinafter *Worldwide Threat Assessment*].

4 *See, e.g.,* Arjun Kharpal, *Power Is 'Up for Grabs': Behind China's Plan to Shape the Future of Next-Generation Tech*, CNBC (Apr. 26, 2020), https://www.cnbc.com/2020/04/27/china-standards-2035-explained.html. On the New Internet Protocol proposal, *see* Madhumita Murgia and Anna Gross, *Inside China's Controversial Mission to Reinvent the Internet*, Financial Times (Mar. 27, 2020), https://www.ft.com/content/ba94c2bc-6e27-11ea-9bca-bf503995cd6f.

5 *Worldwide Threat Assessment*.

6 *See, e.g.*, Christopher Wray, US Dir. Fed. Bureau of Investigation, *The Threat Posed by the Chinese Government and the Chinese Communist Party to the Economic and National Security of the United States*, *Remarks for the Hudson Institute's Video Event: China's Attempt to Influence US Institutions* (July 7, 2020), *in* Archive of Speeches, Fed. Bureau of Investigation, https://www.fbi.gov/news/speeches/the-threat-posed-by-the-chinese-government-and-the-chinese-communist-party-to-the-economic-and-national-security-of-the-united-states (July 7, 2020) (describing the counterintelligence and economic espionage threat from China as "the greatest long-term threat to our nation's information and intellectual property, and to our economic vitality").

7 For instance, see how lack of clarity on US export control rules harmed American companies' ability to stay involved with standards bodies: Ari Schwartz, *Standards Bodies Are under Friendly Fire in the War on Huawei*, Lawfare (May 5, 2020), https://www.lawfareblog.com/standards-bodies-are-under-friendly-fire-war-huawei.

8 ByteDance's algorithms remain a key factor in TikTok's global expansion, for example: Sam Byford, *How China's Bytedance Became the World's Most Valuable Startup*, The Verge (Nov. 30, 2018), https://www.theverge.com/2018/11/30/18107732/bytedance-valuation-tiktok-china-startup.

9 It also conducts influence operations aimed at the Chinese diaspora: Timothy Heath, *Beijing's Influence Operations Target Chinese Diaspora*, War on the Rocks (Mar. 1, 2018), https://warontherocks.com/2018/03/beijings-influence-operations-target-chinese-diaspora.

10 *See* order granting preliminary injunction, https://www.courtlistener.com/recap/gov.uscourts.cand.364733/gov.uscourts.cand.364733.59.0.pdf.

11 Cyberspace Solarium Commission, *Building a Trusted ICT Supply Chain: CSC White Paper #4*, at iii (Oct. 2020), https://drive.google.com/file/d/1efo96fPx5WkOxTiFFY1r5y3lFqdit00C/view [hereinafter *Building a Trusted ICT Supply Chain*].

12 For further discussion of criteria for software and hardware trustworthiness, see Paul Rosenzweig and Claire Vishik, *Trusted Hardware and Software: An Annotated Bibliography*, Lawfare (Oct. 1, 2020), https://www.lawfareblog.com/trusted-hardware-and-software-annotated-bibliography.

13 National Institute of Standards and Technology, *NIST Cloud Computing Standards Roadmap* (July 2013), https://www.nist.gov/system/files/documents/itl/cloud/NIST_SP-500-291_Version-2_2013_June18_FINAL.pdf; International Organization for Standardization, *Information Technology—Security Techniques—Code of Practice for Information Security Controls Based on ISO/IEC 27002 for Cloud Services* (2015), https://www.iso.org/standard/43757.html.

14 *EU Proposes Fresh Alliance with US in Face of China Challenge*, Financial Times (Nov. 29, 2020), https://www.ft.com/content/e8e5cf90-7448-459e-8b9f-6f34f03ab77a.

15 Cyberspace Solarium Commission, *Final Report of the Cyberspace Solarium Commission* (Mar. 2020), https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view.

16 *Building a Trusted ICT Supply Chain*.

About the Authors

Gary Corn is the program director of the Technology, Law & Security Program at the American University Washington College of Law and a nonresident senior fellow at the R Street Institute. He is a retired US Army colonel and previously served in a number of senior positions in the DoD, including as a deputy legal counsel to the chairman of the Joint Chiefs of Staff, and most recently as staff judge advocate (general counsel) to US Cyber Command.

Jennifer Daskal is a professor and faculty director of the Tech, Law & Security Program at American University Washington College of Law, as well as a 2020–21 New America/ASU Future Security Fellow. From 2009 to 2011, she served as counsel to the assistant attorney general for national security at the Department of Justice.

Jack Goldsmith is the Learned Hand Professor of Law at Harvard Law School, a senior fellow at the Hoover Institution, and a cofounder of *Lawfare*. Before coming to Harvard, he served as assistant attorney general, Office of Legal Counsel, from 2003 to 2004 and special counsel to the Department of Defense from 2002 to 2003.

Chris Inglis currently serves as the Naval Academy's Looker Distinguished Visiting Professor of Cyber Studies and as a commissioner on the US Cyberspace Solarium Commission. He previously served at the National Security Agency for twenty-eight years, including more than seven years as its senior civilian and deputy director.

Paul Rosenzweig is a resident senior fellow at the R Street Institute and an adviser to the American Bar Association Standing Committee on National Security Law. He teaches at George Washington University School of Law and was formerly the deputy assistant secretary for policy at the Department of Homeland Security.

Samm Sacks is a cyber policy fellow at New America and a senior fellow at Yale Law School's Paul Tsai China Center. She has worked on China's technology policies for over a decade, both in the national security community and the private sector.

Bruce Schneier is a security technologist and author. He is a fellow at the Berkman Klein Center for Internet and Society at Harvard University; a lecturer in public policy at the Harvard Kennedy School; and a board member of the Electronic Frontier Foundation, Access Now, and the Tor Project. He is the chief of security architecture at Inrupt Inc.

Alex Stamos is the director of the Stanford Internet Observatory and a partner in Krebs Stamos Group. He formerly served as chief security officer at Facebook and Yahoo, was a cofounder of iSEC Partners, and is currently working on election security as a member of the Annan Commission on Elections and Democracy and advising NATO's Cybersecurity Center of Excellence.

Vince Stewart, lieutenant general (ret.), served a distinguished thirty-eight-year career as an intelligence officer in the US Marine Corps, capping his service as the deputy commander of US Cyber Command and, prior to that, as the twentieth director of the Defense Intelligence Agency. Currently, he is the founder and president of Stewart Global Solutions LLC and the chief of innovation and business intelligence at Ankura.

27 26 25 24 23 22 21 7 6 5 4 3 2 1

HOOVER INSTITUTION

The Jean Perkins Foundation Working Group on National Security, Technology, and Law

The Jean Perkins Foundation 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.

Jack Goldsmith is the chair 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.

AMERICAN UNIVERSITY WASHINGTON COLLEGE OF LAW | TECH, LAW & SECURITY PROGRAM

The Technology, Law & Security Program (TLS) is a new initiative at American University Washington College of Law that tackles the challenges and opportunities posed by emerging technology—offering innovative solutions, engaging students, and training the leaders of tomorrow.

Jennifer Daskal is the faculty director of the Technology, Law & Security Program.

Gary Corn is the program director of the Technology, Law & Security Program.

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