A HOOVER INSTITUTION ESSAY

The 'China, Inc.+' Challenge to Cyberspace Norms

ROBERT D. WILLIAMS

Aegis Series Paper No. 1803

Introduction

In September 2015, Chinese President Xi Jinping reached an agreement with US President Barack Obama that the Chinese and American governments would not "conduct or knowingly support" the cyber-enabled theft of trade secrets and confidential business information "with the intent of providing competitive advantages to their companies or commercial sectors."[1] In consenting to this language, what did the respective leaders understand themselves to be committing to? What constitutes "intent" to provide "competitive advantage" to a nation's "commercial sector"? Where is the line between commercial purposes and national security objectives? What degree of control is necessary to impute responsibility to a government rather than a nonstate actor?

The lack of good answers to such questions exposes one aspect of the complexity of efforts to develop and implement norms of state conduct in cyberspace. China provides a particularly illustrative case study of the complexity because its institutional environment does not break down neatly along lines between state/government and nonstate/commercial sectors. Nor is this a straightforward matter of government *ownership*—that is to say, a reflection of the outsized role played by state-owned enterprises (SOEs) in China's economy (a phenomenon that is not unique to China). The challenge is deeper and more fundamental.

One aspect of the challenge is that the usual dichotomy between SOEs and privately owned enterprises (POEs) simply does not hold in the Chinese context. Distinctions between state and market actors, interests, and motivations are often blurred. Numerous firms, regardless of ownership structure, have close connections to state agencies and officials, as well as some (often difficult to define) role in carrying out state policy objectives.[2] The ruling Chinese Communist Party (CCP) is deeply woven into the institutional fabric of Chinese society. Its role in institutional settings can be extremely difficult to disaggregate.[3]

A second and related aspect of the challenge is China's expansive official conception of "national security." Less than three months prior to the September 2015 United States-

I am grateful to Quentin Johnson, Robert Nelson, David Stanton, and Wenqing Zhao for excellent research assistance; and to Jane Chong, Rogier Creemers, Jack Goldsmith, Benjamin Wittes, and participants in the Hoover Institution's National Security, Technology, and Law Working Group at Stanford University for helpful comments.

China cyber agreement, China's National People's Congress (NPC) adopted a National Security Law that codifies a sweeping vision of national security.[4] The legislation defines national security to include the absence of threats to, among other things, "the welfare of the people" and "sustainable economic and social development," as well as "other major national interests."[5] President Xi Jinping has emphasized the need for Party and government officials to adopt a comprehensive national security perspective that incorporates "political, economic, territorial, social and cyber security."[6] On these terms, virtually any objective the CCP might determine to be within the realm of national interests—including economic interests—qualifies in principle as a national security objective.[7] The expansiveness of this conception also opens the possibility that the many Chinese companies that support and carry out the Party-state's priorities cannot be disentangled from the Party-state's capacious national security objectives.

I will refer to these characteristics collectively as the challenge of "China, Inc.+." I borrow the term "China, Inc." from others who have used it to describe the unique role of the state in the Chinese economy.[8] I broaden the concept to include China's expansive understanding of national security—hence the "plus." The "+" moniker also evokes the Chinese government's "internet plus" (互联网+) agenda, which aims to capitalize on the integration of internet and cutting-edge digital technologies into various Chinese industries and government agencies.[9]

The attributes of China, Inc.+ raise vexing questions when considered alongside the PRC's articulated national strategies and policies for cyberspace. Policy initiatives such as "military-civil fusion" blur the distinction between defense and commercial activities and aim to bolster the involvement of Chinese companies and universities in national defense.[10] Thus, the blurred lines between state and nonstate actors, as well as between the national security and commercial priorities of China, Inc.+, are rendered even murkier by what we know from publicly available materials about China's strategy of cyber-power integration.

These challenges complicate efforts to construct workable international norms and rules regarding state conduct in cyberspace. The complexity is borne out in the (perhaps unavoidable) failure of language in recent norm-setting documents to capture the characteristic murkiness of state/market distinctions within Chinese state capitalism. This is particularly so when it comes to norms concerning state responsibility for cyber operations and the prohibition on cyber-enabled theft of trade secrets for commercial advantage—norms recently articulated in the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* and in the 2015 US-China cyber agreement. The blurriness also hints at broader challenges such as achieving consensus with respect to interpretations of sovereignty and the proper scope of government control of the Internet.

Put simply, the China, Inc.+ challenge is about the blending of state and nonstate domains. This has significant and perhaps underappreciated consequences for American policy.

For example, even if we assume perfect attribution of the *source* of every digital breach (a significant challenge in itself) there may be cases in which the deeply integrated nature of China's Party-state apparatus makes it all but impossible to determine with certainty the precise relationship of the operational source to "the state" or the degree of "state control" over that entity.[11] This in turn has implications for international law and norms, as it muddies the waters around both the actors (i.e., whether to attribute state responsibility for a given cyber operation) as well as the conduct itself (i.e., whether the operation is in fact a violation of a norm).

Although the problem sketched here is not necessarily China-specific, it is especially salient in the Chinese context and has important implications for US-China relations and global governance. The future of international relations in cyberspace will not be decided without the participation of the United States and China. It is thus important for American policymakers to be alert to these challenges and to approach future US-China interactions on cyberspace norms with strategies for addressing them.

China, Inc.+

State Capitalism and the Role of the Chinese Communist Party

China's vestigially Leninist system has evolved considerably since the period of "reform and opening up" led by Deng Xiaoping after 1978.[12] Partly owing to the significant economic and legal reforms implemented over the past forty years, China's political system is "neither monolithic nor rigidly hierarchical."[13] Nonetheless, the ruling Chinese Communist Party still "dominates state and society in China, is committed to maintaining a permanent monopoly on power, and is intolerant of those who question its right to rule."[14]

China is a one-party state in which "ultimate power still resides within the Party and not the state."[15] This power is not limited to the Party's control over key appointments in the formal apparatus of state governance and public institutions, or the fact that the People's Liberation Army (PLA) is itself an "armed wing" of the CCP.[16] The Party's presence is pervasive yet subtle; it is embedded in Chinese institutions, organizations, and companies in a manner not adequately accounted for by traditional Western legal constructs.[17] Although the Party no longer seeks to control Chinese citizens' every choice, "it does seek to directly control or heavily influence every sphere of *organized* activity."[18] As former CCP anticorruption czar Wang Qishan candidly stated in a leaked online video: "What's the Communist Party about? You do whatever the party tells you."[19]

The unique embeddedness of the Party-state in China's economy is beginning to receive increased attention in Western legal scholarship. Li-Wen Lin and Curtis Milhaupt refer to the organizational structure of Chinese state capitalism as a "networked hierarchy" in which firms are connected through various formal and informal mechanisms described as "institutional bridging."[20] Entities are linked through "dense networks—not only of

other firms, but also of party and government organs. These networks appear to facilitate information flow from the bottom up as well as from the top down. They foster relational exchange and collaboration on many levels of the production and policy-implementation processes. And they provide high-powered incentives to leaders within the system, because success in business leads to promotion and accompanying rewards in the political realm, and vice versa."[21]

Importantly, the Party-state's role in China's economy is not confined to enterprises in which the state is the dominant shareholder. As professors Milhaupt and Wentong Zheng explain, "Functionally, SOEs and large POEs in China share many similarities in the areas commonly thought to distinguish state-owned firms from privately owned firms: market access, receipt of state subsidies, proximity to state power, and execution of the government's policy objectives."[22] The mechanisms of state control over private enterprise are multiple and subtle. One component, alluded to above, is institutional bridging between organs of the government or CCP and senior executives of large private companies. For example, Milhaupt and Zheng found "ninety-five out of the top one hundred private firms and eight out of the top ten Internet firms whose founder or de facto controller is currently or formerly a member of central or local party-state organizations."[23] Another component is state support of "national champion" private enterprises through major subsidies often thought to be reserved for SOEs.[24] Other mechanisms are extralegal and informal, such as supervision by quasi-governmental industry associations and "the practice of regulators conducting 'interviews' with private firm managers to encourage or compel compliance with policies favored by the government."[25]

Through its appointment power, the Party's Central Organization Department "can decide to rotate individuals between jobs in the state and private sector, across sectors and regions."[26] Moreover, each organization in China with more than three CCP members—whether nominally public or private, domestic or foreign—must establish its own Party committee.[27] In recent years, the CCP has expanded the role of such Party units, including within foreign-invested joint ventures in China.[28] Thus, "throughout the system, the Party has positioned itself like a political panopticon, allowing it to keep an eye on any state or non-state agency, while shielding itself from view at the same time."[29]

According to Professor Mark Wu, the CCP's "deep entrenchment in business, its broad control mechanisms, and its ability to direct resources are all highly distinctive to China."[30] Wu has argued that China's unique economic structure poses a major new challenge to rules of international trade under the World Trade Organization (WTO), which were not designed for China's brand of "economic exceptionalism with intertwined linkages between the state, the Party, and public and private enterprises."[31] He calls this the "China, Inc. challenge" to global trade governance.[32] Expanding on this concept, I will argue that a similarly thorny challenge applies to ongoing efforts to establish mutually acceptable norms for cyberspace.

National Security with Chinese Characteristics

The "plus" component of the China, Inc.+ challenge to cyberspace norms is China's expansive official conception of national security. Chinese government statements and policies have long manifested a broad vision of what falls within the scope of national security and are open to flexible interpretations by Party-state officials. This ambiguity compounds the challenge of delineating normative boundaries between security and nonsecurity objectives in cyberspace as in other domains.

On July 1, 2015, China's National People's Congress (NPC) enacted a National Security Law codifying a sweeping definition of national security.[33] Article 2 of the legislation defines national security as referring to "the relative absence of international or domestic threats to the state's power to govern, sovereignty, unity and territorial integrity, the welfare of the people, sustainable economic and social development, and other major national interests, and the ability to ensure a continued state of security."[34] The statute further provides that:

> National security efforts shall adhere to a comprehensive understanding of national security, make the security of the people their goal, political security their basis, and economic security their foundation; make military, cultural and social security their safeguard and advance international security to protect national security in all areas; build a national security system and follow a path of national security with Chinese characteristics.[35]

Finally, the law contains a familiar instruction to "adhere to the leadership of the Chinese Communist Party" in national security affairs.[36] It articulates a central role for the Party in determining what can and is to be done in the name of national security.[37] On these terms, virtually any objective the CCP might determine to be within the realm of national interests—including economic, social, ideological, and cultural interests—qualifies in principle as a national security objective.

The PRC National Security Law is not an aberration; it is a consolidation. It is one element of a broader effort at "legalization" (法律化) of Party policies and institutions in the wake of the Fourth Plenum of the CCP Central Committee in 2014, which placed "rule according to law" (依法治国) at the center of the Party's governing agenda.[38] The potentially all-encompassing notion of national security codified in the NSL is of a piece with other Chinese laws, policies, and regulations that touch upon national security. For example, China's Criminal Law includes a vague category of crimes against "state or national security," affording broad discretion for Chinese authorities to enforce prohibitions against crimes such as subversion and sedition.[39] Constitutional limits that might constrain the Party-state's exercise of that discretion are weak and not judicially enforceable.[40]

President and CCP General Secretary Xi Jinping articulated the Party-state's far-reaching conception of national security on April 15, 2014, when he chaired the first meeting of

China's newly established National Security Commission.[41] At that meeting, Xi reportedly "specified a national security system that covers safety in 11 fields—politics, territory, military, economy, culture, society, science and technology, information, ecology, nuclear and natural resources."[42] This capacious view was reinforced in February 2017 when Xi, addressing a seminar on national security in Beijing, "called for an overall national security outlook . . . emphasizing the importance of political, economic, territorial, social and cyber security."[43]

The open-ended conception of national security found in the NSL and other PRC policy statements has drawn criticism from foreign businesses and rights advocates alike.[44] Such discussions are largely beyond the scope of this paper.[45] The point here is to emphasize that a definition so broad as to include notions of economic, social, ideological, and cultural security within its ambit, and that fails to further define any of those subcategories, raises significant questions for the establishment of international norms that seek to draw lines between security and nonsecurity purposes as well as between state and nonstate actors and objectives.

Chinese Cyberspace Strategy and Activity

Sketching the General Problem The intertwining of state and nonstate actors as well as security and nonsecurity purposes has important implications for interstate relations in cyberspace. Former State Department legal adviser Harold Koh identified one aspect of the problem in noting that "cyberspace significantly increases an actor's ability to engage in attacks with 'plausible deniability,' by acting through proxies."[46] Several scholars have explored the role of such state "proxies" and sought to delineate categories of state involvement in, and responsibility for, cyber operations aimed at compromising targeted computer networks.[47] Although the difficulties of attribution and of identifying state involvement in cyber operations are not unique to China, the PRC provides a particularly robust illustration of the challenge.

A June 2016 report by the cybersecurity firm FireEye describes the blurring of Chinese state and nonstate cyber operations.[48] FireEye researchers reviewed incidents of network compromise by seventy-two groups that the company "suspect[s] are operating in China or otherwise support Chinese state interests."[49] The firm's meticulous attribution process entails the accumulation of various forms of evidence over time, including the scope and sophistication of operations; specific tactics, techniques, and procedures; and operational details such as efforts at stealth and anonymity.[50] Yet even with these sophisticated methods of tracing the sources of Chinese operations, the report's authors concede that the spectrum of actors involved—from military personnel to patriotic hacktivists—makes it virtually impossible to determine with precision the degrees of state direction or control.[51]

As explained in the FireEye report:

> We have strong indications that the 72 groups we have observed are based in China or otherwise support Chinese interests, although we question whether there is much consistency in the level of state direction or support that each of these groups may receive from the Chinese Government. The Chinese landscape, frequently characterized as monolithic and rigidly state-directed, is composed of a wide range of groups, including government and military actors, contractors, patriotic hackers, and even criminal elements. Occasionally, aligned interests between two types of groups may drive activity that blurs the lines between direct government sponsorship and independent action. For example, during territorial disputes, patriotic hackers may conduct targeting activity that is indistinguishable from that of government forces. As a result, it is often difficult to determine the extent to which activity is directed by the Chinese Government.[52]

The difficulty of distinguishing operations directed by the Chinese government (or CCP) from the work of private hackers at the operational level finds resonance in China's broader official strategy of integration between military and civilian actors in computer network operations. On September 15, 2017, the CCP's leading theoretical journal published an authoritative article articulating Xi's strategic thinking on "building China into a cyber superpower."[53] Included among Xi's priorities is deepening "military-civil fusion" (alternatively translated as "civil-military integration") in the domains of cybersecurity and "informatization."[54] Although the article does not spell out this concept in detail, reviews of Chinese official and semiofficial strategy discourse suggest that it "encompasses a diverse range of activities based on the notion of harnessing the technological and industrial capabilities of the civilian economy to advance defense capabilities"—including the capacity to conduct information warfare.[55] This concerted effort to integrate the civilian and defense industrial base was reinforced in December 2017 with the State Council's release of "Opinions on Deepening the Development of Civil-Military Defense Industry Integration."[56]

One aspect of civil-military integration is the establishment of so-called "information warfare militias," or "cyber militias," in Chinese businesses and universities.[57] According to a US government-commissioned analysis, "since approximately 2002, the PLA has been creating [information warfare] militia units comprised of personnel from the commercial IT sector and academia, and represents an operational nexus between PLA [computer network operations] and Chinese civilian information security (infosec) professionals."[58] These units are embedded "directly within commercial firms throughout China" to capitalize on the expertise and resources of the private sector in accomplishing the PLA's operational goals.[59] They consist of over eight million "hackers, IT companies, scientists, network engineers, foreign language speakers, and others with useful skills" who operate under a command hierarchy with ambiguous connections and accountability to the government and the PLA.[60]

Although concrete evidence of cyber militias' operational purview is scarce, Joe McReynolds has noted that their operations may not be confined to wartime network attack, espionage, or defensive operations. Reviewing the PLA literature on network warfare, McReynolds finds that "outside the context of a full conflict, some PLA writings raise the possibility that during peacetime China may choose to encourage non-military network forces, ranging from militia units to hacktivists, to play a meaningful role in the conduct of low-level network operations."[61] Others have similarly observed that a number of "private sector" corporate intelligence or cybersecurity firms might also fit the profile of advanced persistent threats (APTs)—i.e., entities that target particular organizations for computer network exploitation on a chronic basis, requiring preparatory intelligence to target specific network defenses and gain access to and exfiltrate data.[62]

As the FireEye report suggests, it can be difficult to distinguish government- or Party-linked groups such as those discussed above from patriotic "hacktivists"—online social or political activists that operate independently of the Chinese Party-state but may share its interests and objectives. Such groups may reinforce the PRC's credibility and objectives in international relations but they may also damage the Chinese government's reputation or the receptivity of other governments to cooperating with China.[63] Questions abound concerning the willingness and ability of China's central government and CCP/PLA leadership to exert control over such individuals and groups, and under what circumstances.

Case Studies The foregoing discussion of China's operational landscape points toward the challenge of attributing the identities and motivations of China-based entities engaged in network compromise operations. The challenge is further illustrated by a sampling of reported cyber intrusions by China-based actors.

Operation Aurora In December 2009, Google discovered that its corporate network had been penetrated by an exploitation of a vulnerability in Internet Explorer software.[64] The attacks were subsequently identified as part of a sophisticated operation targeting at least thirty-four companies in the technology, financial, and defense sectors—including Yahoo, Symantec, Adobe, Morgan Stanley, Northrup Grumman, and Dow Chemical—through a variety of vulnerabilities.[65] Media reports, leaked diplomatic cables, and Google's statements on the intrusion suggested that the attacks were a Chinese state-directed operation to infiltrate American corporations in order to obtain politically sensitive information on human rights activists and economically valuable information on strategic sectors.[66]

Night Dragon In February 2011, McAfee published a white paper identifying a series of APT attacks against global energy companies starting in November 2009 which it named "Operation Night Dragon."[67] Like Operation Aurora, the attacks used a variety of means to penetrate company networks, where they seized "sensitive competitive proprietary operations and project-financing information with regard to oil and gas field bids and

operations."[68] The attacks came from several locations in China. McAfee identified a Chinese company that had provided American hosting services to the hackers, but the report did not link them to any particular state or nonstate entity.[69]

Nitro In October 2011, Symantec published a white paper identifying a spear-phishing operation originating in a US-based virtual private server (VPS) owned by a Chinese male located in Hebei.[70] The operation began by targeting human rights organizations but subsequently moved to stealing intellectual property from companies in the chemicals and advanced materials industries.[71] None of the reported evidence linked the attacks to the Chinese government.

Sykipot In January 2012, AlienVault identified a spear-phishing attack targeting the smart cards used by many US government employees, including in the Department of Defense.[72] AlienVault linked several of the attacks, a variant of the Sykipot family of malware, to servers in China, but there was no further reported evidence connecting the attacks to Chinese government or CCP entities.[73]

Luckycat In March 2012, Symantec and Trend Micro released separate white papers on a spear-phishing operation dubbed Luckycat.[74] The operation predominantly targeted Tibetan activists as well as Japan- and India-based targets in the aerospace, energy, engineering, military research, and maritime industries (including information on shipping in the Arabian and South China seas).[75] It was tracked to a former graduate student at Sichuan University who at the time of the reports worked at the internet company Tencent.[76] The Trend Micro report identified an email address used to register one of the Luckycat command-and-control servers to a hacker in the "Chinese underground community" who had "recruited others to join a research project on network attack and defense at the Information Security Institute of the Sichuan University."[77] Neither investigation explicitly linked the student with the Chinese government or cyber militias, although outside experts speculated that the nature of the targets suggested PRC government involvement.[78]

APT1 In February 2013, Mandiant (now FireEye) released a report identifying a threat actor named APT1 as the source of persistent attacks against companies in a range of industries that were economic priorities for the Chinese Party-state.[79] The report concluded the group was government-sponsored and believed to be PLA Unit 61398.[80] In May 2014, the US Department of Justice indicted five members of the unit for computer-enabled economic espionage and related offenses—the first ever charges against a state actor for such hacking.[81]

Register.com In March 2015, the *Financial Times* reported that the FBI was investigating a computer hack directed at Register.com, a domain name registry.[82] The intrusions targeted network and employee passwords but were not known to have caused disruptions or resulted in any theft of the company's client data.[83] The reporting suggested the attacks

may have been part of a Chinese military operation to undermine internet infrastructure, but to date there has been no authoritative public attribution to that effect.[84]

Black Vine In August 2015, Symantec published a white paper identifying an APT, which it termed Black Vine, that was responsible for several operations including a 2014 cyber intrusion against health care provider Anthem that exposed 80 million patient records.[85] The intrusions affected US corporations in industries such as aerospace, energy, and health care, operating through watering-hole attacks on industry websites.[86] These operations appeared to utilize network infrastructure owned by the Beijing-based security company Topsec—whose clients include both government and private entities—but the Symantec report stopped short of establishing a definitive link to the PRC government.[87]

Mofang In May 2016, the Dutch security company Fox-IT published a white paper identifying an APT that had conducted operations closely aligned with China's economic and security interests, such as targeting US federal agencies and Indian defense systems.[88] Compromises carried out by this entity, termed Mofang, included an attack on a Malaysian consortium overseeing investment in an area where the China National Petroleum Corporation hoped to build a pipeline.[89] Based on this evidence, and on characteristics of the intrusions, Fox-IT concluded that the group was "probably government-affiliated," but provided no decisive evidence to that effect.[90]

MenuPass In April 2017, the US Department of Homeland Security's National Cybersecurity and Communications Integration Center (NCCIC) released a report warning of increased activity by a group of actors—generally known as MenuPass, Cloud Hopper, or APT10—against companies in several industries worldwide.[91] Although the report did not implicate China directly, cybersecurity firm FireEye—which has been monitoring the group since at least 2009—believes the group is China-based and operates "in support of Chinese national security goals, including acquiring valuable military and intelligence information as well as the theft of confidential business data to support Chinese corporations."[92]

Alf In October 2017, the Australian government revealed that tens of gigabytes of militarily sensitive but unclassified information had been stolen in a 2016 hack on an Australian defense contractor.[93] The breach, which included American weapons systems such as the F-35 Joint Strike Fighter and P-8 Poseidon surveillance aircraft, had been conducted using tools frequently employed by Chinese hackers.[94] There has been no public attribution, however, and Australia's defense industry minister indicated the attacker "could be a state actor, [or] a non-state actor."[95]

Boyusec In November 2017, the US Department of Justice unveiled an indictment of three Chinese nationals employed by Chinese cybersecurity firm Boyusec, charging them with hacking into the computer systems of Moody's Analytics, Siemens AG, and GPS developer Trimble Inc. to steal confidential business information "for the purpose of commercial

advantage and private financial gain."[96] Boyusec is ostensibly a private firm, but multiple analyses have exposed its links to China's Ministry of State Security.[97] The indictment delineates the commercial sectors serviced by each of the three targeted American firms, emphasizing, for example, that Trimble's GPS technology targeted by the hackers "had no military applications."[98]

The examples outlined above underscore the "shifting and blurred" lines between state and nonstate actors in cyberspace, as well as the difficulty in disentangling "national security" from "commercial" or nongovernmental economic interests.[99] Although these are not entirely new revelations, it is not clear that insights concerning China's unique economic structure and official definition of national security have been fully appreciated in the context of efforts to develop norms of state conduct in cyberspace. This is reflected in the recent history of efforts to achieve consensus on such norms, to which we now turn.

Cyberspace Norms

Commercial Espionage

A central feature of US-China cyber diplomacy has been Washington's effort to persuade Beijing to acknowledge a norm against economic espionage for the benefit of commercial firms.[100] The putative norm gained attention following the US Department of Justice's May 2014 indictment of five PLA officers for allegedly hacking into American companies and stealing information to benefit their competitors in China.[101] It came to a head in September 2015 when President Obama and President Xi reached an agreement that "neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors."[102] The norm seemed to have been bolstered when this linguistic formulation gained the support of G-20 leaders at their November 2015 summit.[103] And the agreement was reaffirmed by Washington and Beijing as recently as October 2017.[104]

Private sector analyses and statements by US officials indicate that the raw volume of intellectual property and trade secret theft emanating from China has in fact declined since the 2014 PLA indictment and the 2015 commercial espionage agreement, somewhat reducing bilateral tensions on the issue.[105] Some have cited this as evidence that China is "complying" with the 2015 cyber agreement.[106] But questions remain about the norm's robustness—including what types of cybertheft its ambiguous terms actually ruled out.

For present purposes, we can assume the language of the agreement accurately reflects what was intended by the negotiators and set aside the debate over the degree of compliance with the agreement to date.[107] What exactly is the significance of this normative commitment for China—particularly given the nature of China, Inc.+? Is the agreement limited to government entities, leaving a massive loophole for the Party? Surely the PLA—an arm of

the CCP, not the government—is not exempt from this understanding. But what about SOEs and POEs enmeshed in dense networks and linkages with institutions of government and of the Party? What is the scope of the "commercial" sector in China?

Beyond the question of which entities are covered by the commitment, what conduct does it proscribe? PRC law and Xi's own rhetoric make clear that China's official notion of national security is all-encompassing—certainly comprehensive enough to include goals of economic development and industrial advancement. If Party leaders believe that providing stolen commercial secrets to Chinese companies supports these objectives, it is not clear that this would violate the "intent" to provide competitive advantages in the marketplace.

The persistence of such questions and the weakness of the commercial espionage norm were further exposed in November 2017, when (as noted above) the US Department of Justice unsealed an indictment of three Chinese nationals employed by Chinese cybersecurity firm Boyusec.[108] The suspects were charged with hacking into the computer systems of Moody's Analytics, Siemens AG, and Trimble Inc. to steal confidential business information "for the purpose of commercial advantage and private financial gain."[109] Boyusec is ostensibly a private firm, but cybersecurity analysts have exposed its links to China's Ministry of State Security.[110] The indictment delineates the commercial sectors serviced by each of the three targeted American firms, emphasizing, for example, that Trimble's GPS technology targeted by the hackers "had no military applications."[111] The Boyusec indictment thus suggests that Beijing is either violating the 2015 agreement or exploiting its ambiguities, thus exposing the weakness of the norm against commercial cybertheft.

To be sure, the frailty of this norm is not limited to the challenge of China, Inc.+. The norm has also come under pressure in the United States from those who argue that national and economic security are inseparable.[112] For example, shortly before the Justice Department announced the Boyusec indictment, President Donald Trump tweeted that "economic security is not merely RELATED to national security—economic security IS national security."[113] Others have argued that the private sector in the United States already fulfills a quasi-governmental role on important cybersecurity issues, while the US government sometimes behaves more like a market participant than a regulator.[114] In the future, it is possible that the US conditions giving rise to the norm—particularly the traditional distinction between economic and classical security concerns—may erode "under conditions of pervasive collaboration between the market and the state in the delivery of national security," to the point where "the norm may well fall prey to its generous exceptions."[115]

In any event, in the eyes of American policymakers, the commercial espionage norm restricts a decidedly narrow category of conduct. As former director of national intelligence James Clapper put it, "What we do not do is . . . use our foreign intelligence capabilities to steal the trade secrets of foreign companies on behalf of—or give the intelligence we

collect to—US companies to enhance their international competitiveness or increase their bottom line."[116] This suggests that the touchstone for what is permissible is whether a state-sponsored actor has the *intent* to enhance the *market competitiveness* of a *private* company. The distinctive features of China, Inc.+ suggest this is a needle the Chinese Party-state may not be willing or able to thread. And it should give pause about whether Chinese officials have a similar understanding of what is ruled out under the 2015 cyber agreement.

State Responsibility

What is the difference between a patriotic "hacktivist" operating on her own accord and a state-sponsored campaign of cyberespionage? The second edition of the *Tallinn Manual on the International Law Applicable to Cyber Operations* (*Tallinn 2.0*), released to the public in February 2017, seeks to answer such questions.[117] Despite its admirable ambition and detailed reasoning, however, it is open to question whether the answers *Tallinn 2.0* provides reflect state practice and *opinio juris* with respect to the challenge of China, Inc.+.

Prepared by an International Group of Experts convened under the NATO Cooperative Cyber Defense Center of Excellence (including one participant from Mainland China), *Tallinn 2.0* purports to state *lex lata*—i.e., international law as it currently exists.[118] A section on the law of international responsibility deals with the challenge of attribution to state actors. The distinction between state and nonstate actors is crucial in the law of state responsibility because "international law by and large does not regulate cyber operations conducted by non-State actors, such as private individuals or companies."[119] Consequently, this limits the range of internationally lawful responses a state can engage in (e.g., countermeasures) when it is the target of cyber operations by nonstate actors.[120]

Rules 15 and 17 of *Tallinn 2.0* address the attribution of cyber operations to states. Cyber operations are attributable to states when (1) they are conducted by "organs of a State, or by persons empowered by domestic law to exercise elements of governmental authority," or (2) when a nonstate actor engages in a cyber operation (a) "pursuant to [a state's] instructions or under its direction or control," or (b) that is "acknowledge[d] and adopt[ed]" by the state as its own.[121]

The Experts' commentary to Rule 15 clarifies that the touchstone for the "state organ" analysis is whether the entity in question has that status under the internal law of the state, such that it sits somewhere within the governmental hierarchy.[122] Where the entity does not formally have such status, characterizing it as a state organ must be exceptional. For example, "the mere fact of State ownership is not alone sufficient to characterise a corporation as an organ of a State."[123] Similarly, "the mere fact that a cyber operation has been launched or otherwise originates from governmental cyber infrastructure, or that malware used against hacked cyber infrastructure is designed to 'report back' to another State's governmental cyber infrastructure, is usually insufficient evidence for attributing the

operation to that State."[124] Instead, an entity's acts are attributable to a state when they are of a "governmental character" and the entity is "empowered by the State to carry out such acts."[125]

A second route to state attribution obtains when nonstate actors act "on the instructions of, or under the direction or control of, [a] State in carrying out the conduct."[126] The question of what degree of control is sufficient to attribute the cyber activity of an ostensibly nonstate actor to a state has been a subject of much debate.[127] *Tallinn* opts for the "effective control" standard employed by the International Court of Justice in the *Nicaragua* and *Genocide* judgments, as distinct from the lower threshold of "overall control" applied in the context of assessing whether an armed conflict is an "international armed conflict."[128] Under the effective control standard, "a State is in 'effective control' of a particular cyber operation by a non-State actor whenever it is the State that determines the execution and course of the specific operation and the cyber activity engaged in by the non-State actor is an 'integral part of that operation.' Effective control includes both the ability to cause constituent activities of the operation to occur, as well as the ability to order the cessation of those that are underway."[129]

On this account, attribution is not established where a state provides "general support" or "encouragement" for a nonstate actor or its cyber operations.[130] A state that "merely supplement[s] a non-State actor's cyber activities or assum[es] responsibility for performing a particular function" is not to be construed as having "effective control."[131] By way of example, the "mere provision of malware by a State to a non-State actor does not amount, without more, to effective control . . . ."[132]

Applied to China, Inc.+, this legal parsing prompts the question: What is "the state"? As discussed above, the CCP is enmeshed in China's economy and exercises control at numerous formal and informal points of contact throughout the system. As a result, many Chinese POEs share attributes often thought to characterize SOEs, including "market access, receipt of state subsidies, proximity to state power, and execution of the government's policy objectives."[133] At what point can the execution of government policy objectives be said to reflect nonstate action under the "direction" or "control" of the state? *Tallinn 2.0* indicates that general policy guidance and even provision of hacking resources to nonstate entities is insufficient to establish "effective control." But *from whom* and *to whom* are the relevant interactions? Is the "state" to be understood as the formal apparatus of government, or should we think of the "Party-state" as the relevant locus of authority? Could a Party committee embedded in a private firm be said to exercise "effective control" over operations carried out by that firm's employees? Setting aside the infeasibility of third-party adjudication, what evidence would be considered acceptable, for purposes of norm-adherence, to make such a showing?

Professors Michael Schmitt and Liis Vihul have sought to assuage such concerns by suggesting that a standard of "clear evidence" applies to state attribution, not absolute certainty or "beyond a reasonable doubt."[134] They offer the example of the Mandiant report concerning the hacking activities of PLA Unit 61398, which asserted that the unit acted "with the full knowledge and cooperation of the Chinese government."[135] According to Schmitt and Vihul, "Some have challenged [the Mandiant report's] assertion, but so long as the victim states acted with reasonable certainty based on clear evidence that China is behind the operations, they would have been within the bounds of the law in responding through demands for cessation, claims of reparations, or countermeasures."[136] Perhaps as applied to the PLA, the question of who represents "China" in this equation is clear enough. But at what point do linguistic turns of phrase such as the "Chinese government" and "China" fail to capture the reality of China, Inc.+?

The point here is not to call into question whether the principles carefully articulated in the *Tallinn Manual* accurately represent *lex lata* or in fact reflect *lex ferenda* (i.e., what the International Group of Experts believes the law should be). It is instead to suggest that norms or putative rules of law that turn on state/nonstate distinctions are hard-pressed to account for the fluidity of such distinctions and that this is particularly evident with respect to China's unique brand of state capitalism.

In conclusion, it bears noting that the *Tallinn Manual* is illustrative but hardly alone in exemplifying this tension. Since 2004, China has sent representatives to participate in the norm-setting efforts of the UN Group of Government Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security.[137] In June 2013, for the first time, the GGE reached agreement that "international law, and in particular the Charter of the United Nations, is applicable" to cyberspace.[138] The next GGE report, released in July 2015, went a step further. China agreed to a number of US-backed norms, including a rule of state responsibility under which, among other things, "States must not use proxies to commit internationally wrongful acts using [information and communication technologies], and should seek to ensure that their territory is not used by non-State actors to commit such acts."[139] Although ostensibly a great achievement, the 2015 report's lack of further elucidation as to how "state responsibility" is determined suggests there is room for widely differing interpretations of the norm.

The collapse of the next round of the GGE in June 2017 reinforces this conclusion. The effort to produce a consensus GGE report apparently failed when a small group of countries, including China, rejected three legal principles in the proposed text—including states' right of self-defense under the UN Charter and the right to respond to internationally wrongful acts.[140] The US State Department representative to the GGE process minced no words in articulating her frustration: "I am coming to the unfortunate conclusion that those who are unwilling to affirm the applicability of these international legal rules and principles believe their States are free to act in or through cyberspace to achieve their political ends

with no limits or constraints on their actions."[141] Whether hyperbole or not, this sentiment highlights the distance still to be traveled in reaching consensus on norms of state responsibility in cyberspace.

Conclusion

This paper has sought to explain two distinctive features of China's governance model that pose challenges to the construction of international cyberspace norms: the uniquely embedded and intertwined nature of the Party-state in China's economy and the expansive conception of national security reflected in Chinese laws and policy statements. As relevant to the US-China relationship, I have considered two manifestations of this "China, Inc.+" challenge: to the norm against state-sponsored commercial espionage and to the law of state responsibility for cyber operations. It is likely, however, that the challenge extends to other areas of norm-construction—for example, putative legal limits on states' sovereign rights to regulate the internet within their borders.[142] It may also extend to debates over the definition of "critical infrastructure," which international norms aim to protect from state-sponsored cyberattack.[143]

US policymakers must be sensitive to these complexities and may need new analytical paradigms that transcend rather than resolve them. In responding to offensive cyber operations, for example, the US government would do well to develop a "spectrum of national responsibility" for attributing cyber operations that takes account of the Chinese context.[144] This will require, among other things, investing the necessary resources to obtain a nuanced understanding of the evolving role of the Party-state in various Chinese institutions.

One opportunity for improving such understanding is through bilateral mechanisms such as the US-China Law Enforcement and Cybersecurity Dialogue (LECD).[145] If appropriately resourced and staffed, this dedicated Track I forum could facilitate improved transparency around amorphous notions of state/nonstate actors and security/nonsecurity objectives. Progress will not be made without establishing an atmosphere of mutual trust and candor in such discussions. But if Chinese interlocutors were able to provide frank responses about their interpretations of the appropriate limits on state conduct, this could open new opportunities for the development of more robust bilateral and international norms.[146] Similarly, American stakeholders should prepare to be challenged on their own (perhaps indeterminate) views on questions of commercial espionage, state responsibility, and the like. Neither China nor any other state will acquiesce to boundaries on its conduct while allowing the United States to maintain strategic ambiguity concerning its own.

Ultimately, bilateral dialogues such as the LECD and multilateral norm-setting initiatives such as the GGE cannot substitute for signaling and deterrence strategies. The United

States should continue to test other means of communicating its positions on cyberspace norms that maintain clarity and consistency. One element of such an approach may be the "naming-and-shaming" exemplified in the Department of Justice's recent indictment of the Boyusec hackers, discussed above. As in the case of the 2014 PLA indictment, the Boyusec defendants are almost certainly currently located in China, and it is highly unlikely they will be extradited to stand trial in the United States. As in 2014, however, prosecution is not the point. The move is intended to send a message to the Chinese government: (1) Washington is not happy about China's ongoing violation of the 2015 Obama-Xi cyber agreement, particularly (2) the use of nominally private entities as proxies to carry out state objectives; and (3) if Boyusec is going to hold itself out as "private," then it will be treated under US law like any other private enterprise.

Time will tell whether measures such as the Boyusec indictment produce concrete results. That the indictment was reportedly unsealed only after diplomatic efforts with Beijing failed suggests the multiple tools available for Washington to signal its normative positions.[147] A possible next phase in the approach could include a package of sanctions against specific Chinese entities that continue to violate the commercial espionage norm.[148] To be sure, such an approach will not guarantee that the American and Chinese governments will move closer to agreement on the meaning of such norms. In the short term, it may even exacerbate tensions in an already delicate bilateral relationship. But the more that norms around state conduct in cyberspace remain at the forefront of US-China interactions, the greater the cause for hope that differences can eventually be bridged between the most powerful actors defining international relations in cyberspace for the twenty-first century.

NOTES

1 "Full Text: Outcome List of President Xi Jinping's State Visit to the United States," People's Republic of China Ministry of Foreign Affairs, September 26, 2015, accessed February 9, 2018, www.fmprc.gov.cn/mfa_eng/zxxx_662805/t1300771.shtml (English); 习近平主席对美国进行国事访问中方成果清单, accessed February 9, 2018, www.mfa.gov.cn/chn//gxh/zlb/smgg/t1300767.htm (Chinese) ("中美双方同意，各自国家政府均不得从事或者在知情情况下支持网络窃取知识产权，包括贸易秘密，以及其他机密商业信息，以使其企业或商业行业在竞争中处于有利地位。"). See also "Fact Sheet: President Xi Jinping's State Visit to the United States," The White House, September 25, 2015, accessed February 9, 2018, https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states. The agreement was reaffirmed in October 2017. US Department of Justice, "First U.S.-China Law Enforcement and Cybersecurity Dialogue: Summary of Outcomes," news release, October 6, 2017, accessed February 9, 2018, https://www.justice.gov/opa/pr/first-us-china-law-enforcement-and-cybersecurity-dialogue.

2 Curtis J. Milhaupt and Wentong Zheng, "Beyond Ownership: State Capitalism and the Chinese Firm," *Georgetown Law Journal* 103 (2015): 665, 668–69.

3 Similarly, the extent of central versus local Party control can be difficult to determine.

4 Chun Han Wong, "China Adopts Sweeping National-Security Law," *Wall Street Journal*, July 1, 2015, accessed February 9, 2018, https://www.wsj.com/articles/china-adopts-sweeping-national-security-law-1435757589.

5 National Security Law of the People's Republic of China, art. 2, adopted July 1, 2015, accessed February 9, 2018, www.chinalawtranslate.com/2015nsl/?lang=en (unofficial English translation); accessed February 9, 2018, http://news.xinhuanet.com/politics/2015-07/01/c_1115787801.htm (Chinese).

6 "Xi Calls for Overall National Security Outlook," *Xinhua*, February 17, 2017, accessed February 9, 2018, http://news.xinhuanet.com/english/2017-02/17/c_136065190.htm (English); see also 习近平主持召开国家安全工作座谈会 [Xi Jinping presides over national security work forum], *Xinhua*, February 17, 2017, accessed February 9, 2018, http://news.xinhuanet.com/politics/2017-02/17/c_1120486809.htm (Chinese).

7 National Security Law of China, art. 4 ("Adhere to the leadership of the Chinese Communist Party in national security matters . . . .").

8 Mark Wu, "The 'China, Inc.' Challenge to Global Trade Governance," *Harvard International Law Journal* 57 (2016): 261, 323. Wu describes "China, Inc." as "a form of economic exceptionalism with intertwined linkages between the state, the Party, and public and private enterprise." For an earlier use of the term to describe the Chinese economy, see Ted Fishman, *China, Inc.: How the Rise of the Next Superpower Challenges America and the World* (New York: Scribner, 2006).

9 "China Unveils Internet Plus Action Plan to Fuel Growth," *Xinhua*, July 4, 2015, accessed February 9, 2018, http://english.gov.cn/policies/latest_releases/2015/07/04/content_281475140165588.htm; "Internet Plus," State Council of the People's Republic of China, accessed February 9, 2018, http://english.gov.cn/2016special/internetplus.

10 Greg Levesque and Mark Stokes, "Blurred Lines: Military-Civil Fusion and the 'Going Out' of China's Defense Industry," *Pointe Bello*, December 2016; Robert Sheldon and Joe McReynolds, "Civil-Military Integration and Cybersecurity: A Study of Chinese Information Warfare Militias," in *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, ed. Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron (Oxford, UK: Oxford University Press, 2015), 188.

11 E.g., Lily Hay Newman, "Hacker Lexicon: What is the Attribution Problem?" *Wired*, December 24, 2016, accessed February 9, 2018, https://www.wired.com/2016/12/hacker-lexicon-attribution-problem.

12 Jonathan R. Stromseth, Edmund J. Maleskev, and Dimitar D. Gueorguiev, *China's Governance Puzzle: Enabling Transparency and Participation in a Single-Party State* (Cambridge, UK: Cambridge University Press, 2017). See also, e.g., "China's Path toward Opening Up Its Financial System," *Bloomberg*, November 10, 2017, accessed February 9, 2018, https://www.bloomberg.com/news/articles/2017-11-10/china-s-path-toward-opening-up-its-financial-system-a-timeline.

13 Susan V. Lawrence and Michael F. Martin, "Understanding China's Political System," Congressional Research Service, March 20, 2013: 1, accessed February 10, 2018, https://fas.org/sgp/crs/row/R41007.pdf.

14 Lawrence and Martin, "Understanding China's Political System," Summary.

15 Wu "China, Inc. Challenge," 280.

16 Lawrence and Martin, "Understanding China's Political System," 6, 11.

17 On the role of the CCP, see Richard McGregor, *The Party: The Secret World of China's Communist Rulers* (London: Penguin, 2010).

18 Arthur R. Kroeber, *China's Economy: What Everyone Needs to Kno*w (Oxford: Oxford University Press, 2016), 3.

19 Chris Buckley, "Xi Jinping, Seeking to Extend Power, May Bend Retirement Rules," *New York Times*, March 2, 2017, accessed February 10, 2018, https://www.nytimes.com/2017/03/02/world/asia/xi-jinping-china-retirement-rules.html.

20 Li-Wen Lin and Curtis J. Milhaupt, "We Are the (National) Champions: Understanding the Mechanisms of State Capitalism in China," *Stanford Law Review* 65 (2013): 697, 707–8.

21 Lin and Milhaupt, “National Champions,” 707.

22 Milhaupt and Zheng, “Beyond Ownership,” 668.

23 Milhaupt and Zheng, “Beyond Ownership,” 684.

24 Milhaupt and Zheng, “Beyond Ownership,” 685.

25 Milhaupt and Zheng, “Beyond Ownership,” 687.

26 Wu, “China, Inc. Challenge,” 280.

27 Wu, “China, Inc. Challenge,” 281.

28 E.g., Lucy Hornby, “Communist Party Asserts Control Over China Inc,” *Financial Times*, October 3, 2017, accessed February 10, 2018, https://www.ft.com/content/29ee1750-a42a-11e7-9e4f-7f5e6a7c98a2; Michael Martina, “Exclusive: In China, the Party’s Push for Influence Inside Foreign Firms Stirs Fears,” *Reuters*, August 24, 2017, accessed February 10, 2018, https://www.reuters.com/article/us-china-congress-companies/exclusive-in-china-the-partys-push-for-influence-inside-foreign-firms-stirs-fears-idUSKCN1B40JU; Chun Han Wong and Eva Dou, “Foreign Companies in China Get a New Partner: The Communist Party,” *Wall Street Journal*, October 29, 2017, accessed February 10, 2018, https://www.wsj.com/articles/foreign-companies-in-china-get-a-new-partner-the-communist-party-1509297523.

29 McGregor, *The Party*, 17.

30 Wu, “China, Inc., Challenge,” 282.

31 Wu, “China, Inc., Challenge,” 323.

32 Wu, “China, Inc., Challenge,” 323.

33 Edward Wong, “China Approves Sweeping Security Law, Bolstering Communist Rule,” *New York Times*, July 1, 2015, accessed February 10, 2018, https://www.nytimes.com/2015/07/02/world/asia/china-approves-sweeping-security-law-bolstering-communist-rule.html.

34 National Security Law, art. 2.

35 National Security Law, art. 3.

36 National Security Law, art. 4.

37 National Security Law, art. 6, 16.

38 “CCP Central Committee Decision Concerning Some Major Questions in Comprehensively Advancing Governing the Country According to Law” [Fourth Plenum Decision] (中共中央关于全面推进依法治国若干重大问题的决定), October 29, 2014, accessed February 10, 2018, http://cpc.people.com.cn/n/2014/1029/c64387-25927606.html (Chinese); accessed February 10, 2018, https://chinacopyrightandmedia.wordpress.com/2014/10/28/ccp-central-committee-decision-concerning-some-major-questions-in-comprehensively-moving-governing-the-country-according-to-the-law-forward (unofficial English translation).

39 Jacques deLisle, “Security First? Patterns and Lessons from China’s Use of Law to Address National Security Threats,” *Journal of National Security Law & Policy* 4 (2010): 397, 401.

40 DeLisle, “Security First?” 405.

41 Shannon Tiezzi, “China’s National Security Commission Holds First Meeting,” *The Diplomat*, April 16, 2014, accessed February 10, 2018, http://thediplomat.com/2014/04/chinas-national-security-commission-holds-first-meeting.

42 “China to Follow Specific National Security Strategy,” *Xinhua*, April 16, 2014, accessed February 10, 2018, www.china.org.cn/opinion/2014-04/17/content_32121236.htm (English); 习近平：坚持总体国家安全观 走中国特色国家安全道路

[Xi Jinping: Adhere to a comprehensive perspective of national security and follow the path of national security with Chinese characteristics], *People's Daily*, April 16, 2014, accessed February 10, 2018, http://cpc.people.com.cn/n/2014/0416/c64094-24900492.html (Chinese).

43 "Xi Calls for Overall National Security Outlook," *Xinhua*, February 17, 2017, accessed February 10, 2018, http://news.xinhuanet.com/english/2017-02/17/c_136065190.htm.

44 Chun Han Wong, "China Adopts Sweeping National-Security Law."

45 Also noteworthy but beyond the present scope are the debates on states' invocation of national security in other contexts such as the GATT/WTO. See, e.g., Roger P. Alford, "The Self-Judging WTO Security Exception," *Utah Law Review* 2011, no. 3 (2011): 697, 704–8.

46 Harold H. Koh, "International Law in Cyberspace," *Harvard International Law Journal* 54 (2012): 1, 8, accessed February 10, 2018, www.harvardilj.org/wp-content/uploads/2012/12/Koh-Speech-to-Publish1.pdf.

47 See, e.g., Jason Healey, "The Spectrum of National Responsibility for Cyberattacks," *Brown Journal of World Affairs* 18, no. 1 (Fall/Winter 2011): 43; Tim Maurer, "'Proxies' and Cyberspace," *Journal of Conflict and Security Law* 21 (December 17, 2016): 383.

48 "Red Line Drawn: China Recalculates Its Use of Cyber Espionage," FireEye Special Report, June 2016, accessed February 10, 2018, https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf.

49 FireEye Red Line Report, 3.

50 FireEye Red Line Report, 12.

51 FireEye Red Line Report, 15.

52 FireEye Red Line Report, 15.

53 Theoretical Studies Center Group, Cyberspace Administration of China, 深入贯彻习近平总书记网络强国战略思想 扎实推进网络安全和信息化工作 [Deepening the implementation of General Secretary Xi Jinping's strategic thinking on building China into a cyber superpower: Steadily advancing cybersecurity and informatization work], *Qiushi*, September 15, 2017, accessed February 10, 2018, www.qstheory.cn/dukan/qs/2017-09/15/c_1121647633.htm (Chinese); "China's Strategic Thinking on Building Power in Cyberspace: A Top Party Journal's Timely Explanation Translated," *New America*, September 25, 2017, accessed February 10, 2018, https://www.newamerica.org/cybersecurity-initiative/blog/chinas-strategic-thinking-building-power-cyberspace (unofficial English translation).

54 Theoretical Studies Center Group, "Xi Jinping's strategic thinking"; *New America*, "China's Strategic Thinking."

55 Sheldon and McReynolds, " "Civil-Military Integration and Cybersecurity," 188–89.

56 国务院办公厅关于推动国防科技工业军民融合深度发展的意见 [General Office of the State Council Opinions on Deepening the Development of Civil-Military Defense Industry Integration], December 4, 2017, accessed February 10, 2018, www.gov.cn/zhengce/content/2017-12/04/content_5244373.htm; "China to Allow More Private Capital in Military Industry," *Xinhua*, December 4, 2017, accessed February 10, 2018, http://news.xinhuanet.com/english/2017-12/04/c_136800201.htm.

57 Sheldon and McReynolds, "Civil-Military Integration and Cybersecurity," 207; Mikk Raud, "China and Cyber: Attitudes, Strategies, Organisation," NATO Cooperative Cyber Defence Centre of Excellence, 2016, 26–27, accessed February 10, 2018, https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_CHINA_092016_FINAL.pdf.

58 Bryan Krekel, "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation," report for the US-China Economic and Security Review Commission, Northrop Grumman,

October 9, 2009, 33, accessed February 10, 2018, https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-030.pdf.

59 Krekel, "China Capability for Cyber Warfare and Computer Network Exploitation," 33.

60 Raud, "China and Cyber," 26.

61 Joe McReynolds, "China's Military Strategy for Network Warfare," in *China's Evolving Military Strategy*, ed. Joe McReynolds (Washington, DC: Jamestown Foundation, 2016), 213, 240.

62 Jon R. Lindsay and Tai Ming Cheung, "From Exploitation to Innovation: Acquisition, Absorption, and Application," in *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, ed. Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron (Oxford: Oxford University Press, 2015), 51, 61, 64.

63 Raud, "China and Cyber," 26.

64 Kim Zetter, "Google Hack Attack Was Ultra Sophisticated, New Details Show," *Wired*, January 14, 2010, accessed February 10, 2018, https://www.wired.com/2010/01/operation-aurora.

65 Zetter, "Google Hack Attack"; Ariana Eunjung Cha and Ellen Nakashima, "Google China Cyberattack Part of Vast Espionage Campaign, Experts Say," *Washington Post*, January 14, 2010, accessed February 10, 2018, www.washingtonpost.com/wp-dyn/content/article/2010/01/13/AR2010011300359.html.

66 "A New Approach to China," Google Official Blog, January 12, 2010, accessed February 10, 2018, https://googleblog.blogspot.com/2010/01/new-approach-to-china.html; Tim Lister, "WikiLeaks: Chinese Attacks on Google Came from the Top," CNN, December 6, 2010, accessed February 10, 2018, www.cnn.com/2010/WORLD/asiapcf/12/05/wikileaks.china.google/index.html; Cha and Nakashima, "Google China Cyberattack"; Zetter, "Google Hack Attack."

67 "Global Energy Cyberattacks: 'Night Dragon,'" McAfee white paper, February 11, 2011, 3–4, 18, accessed February 10, 2018, https://github.com/kbandla/APTnotes/blob/master/2011/wp-global-energy-cyberattacks-night-dragon.pdf.

68 "McAfee: Oil and Gas Firms Targeted with Night Dragon Cyberattacks," PennEnergy, February 10, 2011, accessed February 10, 2018, www.pennenergy.com/articles/pennenergy/2011/02/mcafee--oil-and-gas.html.

69 McAfee, "Night Dragon," 3–4, 18.

70 Eric Chien and Gavin O'Gorman, "The Nitro Attacks: Stealing Secrets from the Chemical Industry," Symantec Security Response, 2011, accessed February 10, 2018, https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_nitro_attacks.pdf.

71 Chien and O'Gorman, "Nitro Attacks," 1–2.

72 Jaime Blasco, "Sykipot Variant Hijacks DOD and Windows Smart Cards," AlienVault Blog, January 12, 2012, accessed February 10, 2018, https://www.alienvault.com/blogs/labs-research/sykipot-variant-hijacks-dod-and-windows-smart-cards.

73 Blasco, "Sykipot Variant Hijacks DOD"; Jaime Blasco, "Are the Sykipot's Authors Obsessed with Next Generation US Drones?" AlienVault Blog, December 20, 2011, accessed February 10, 2018, https://www.alienvault.com/blogs/labs-research/are-the-sykipots-authors-obsessed-with-next-generation-us-drones; Vikram Thakur, "The Sykipot Attacks," Symantec Official Blog, December 8, 2011, accessed February 10, 2018, https://www.symantec.com/connect/blogs/sykipot-attacks.

74 "The Luckycat Hackers," Symantec Security Response, 2012, accessed February 10, 2018, https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/luckycat-hackers-12-en.pdf; "Luckycat Redux: Inside an APT Campaign with Multiple Targets in India and Japan," Trend Micro research paper, 2012, accessed February 10, 2018, https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp_luckycat_redux.pdf.

75 Trend Micro, “Luckycat Redux,” 1; Symantec, “Luckycat,” 2.

76 Nicole Perlroth, “Case Based in China Puts a Face on Persistent Hacking,” *New York Times*, March 29, 2012, accessed February 10, 2018, www.nytimes.com/2012/03/30/technology/hacking-in-asia-is-linked-to-chinese-ex-graduate-student.html.

77 Trend Micro, “Luckycat Redux,” 2.

78 Perlroth, “Case Based in China.”

79 “APT1: Exposing One of China’s Cyber Espionage Units,” Mandiant, 2013, accessed February 10, 2018, https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf.

80 Mandiant, “APT1,” 3.

81 US Department of Justice, “U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage,” news release, May 19, 2014, accessed February 10, 2018, https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor; Michael S. Schmidt and David E. Sanger, “5 in China Army Face U.S. Charges of Cyberattacks,” *New York Times*, May 19, 2014, accessed February 10, 2018, https://www.nytimes.com/2014/05/20/us/us-to-charge-chinese-workers-with-cyberspying.html?_r=0.

82 Gina Chon, Hannah Kuchler, and Kara Scannell, “FBI Probes Possible China Military Involvement in Cyber Attack,” *Financial Times*, March 18, 2015, accessed February 10, 2018, https://www.ft.com/content/ab5d5736-cd24-11e4-b5a5-00144feab7de.

83 Chon, Kuchler, and Scannell, “FBI Probes Possible China Military Involvement.”

84 Chon, Kuchler, and Scannell, “FBI Probes Possible China Military Involvement.” See also Elizabeth Shim, “FBI Looking into Chinese Military Involvement in Cyber Hack of U.S. Company,” UPI, March 18, 2015, accessed February 10, 2018, https://www.upi.com/Top_News/World-News/2015/03/18/FBI-looking-into-Chinese-military-involvement-in-cyber-hack-of-US-company/2531426688682.

85 Jon DiMaggio, “The Black Vine Cyberespionage Group,” Symantec Security Response, August 6, 2015, 5, accessed February 10, 2018, www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-black-vine-cyberespionage-group.pdf.

86 DiMaggio, “The Black Vine,” 11–14.

87 DiMaggio, “The Black Vine,” 14–15.

88 Yonathan Klijnsma, “Mofang: A Politically Motivated Information Stealing Adversary,” Fox-IT, May 17, 2016, accessed February 10, 2018, https://www.fox-it.com/en/wp-content/uploads/sites/11/Fox-IT_Mofang_threatreport_tlp-white.pdf.

89 Klijnsma, “Mofang,” 18.

90 Klijnsma, “Mofang,” 5, 6. See also Kim Zetter, “Revealed: Yet Another Group Hacking for China’s Bottom Line,” *Wired*, June 14, 2016, accessed February 10, 2018, https://www.wired.com/2016/06/revealed-yet-another-chinese-group-hacking-countrys-economic-bottom-line.

91 US Department of Homeland Security, “Incident Report: Intrusions Affecting Multiple Victims Across Multiple Sectors,” incident report, National Cybersecurity and Communications Integration Center, April 27, 2017, accessed February 10, 2018, https://www.us-cert.gov/sites/default/files/publications/IR-ALERT-MED-17-093-01C-Intrusions_Affecting_Multiple_Victims_Across_Multiple_Sectors.pdf.

92 “APT10 (MenuPass Group): New Tools, Global Campaign Latest Manifestation of Longstanding Threat,” FireEye iSight Intelligence, April 6, 2017, accessed February 10, 2018, https://www.fireeye.com/blog/threat-research/2017/04/apt10_menupass_grou.html.

93 "Australia Jet and Navy Data Stolen in 'Extensive' Hack," BBC, October 12, 2017, accessed February 10, 2018, www.bbc.com/news/world-australia-41590614.

94 BBC, "Australia Jet and Navy Data Stolen."

95 BBC, "Australia Jet and Navy Data Stolen"; see also "Secret Files on Jets and Navy Ships Stolen in 'Extensive and Extreme' Hack," *The Guardian*, October 11, 2017, accessed February 10, 2018, https://www.theguardian.com/australia-news/2017/oct/12/secret-files-on-jets-and-navy-ships-stolen-in-extensive-and-extreme-hack.

96 Jack Goldsmith and Robert D. Williams, "The Chinese Hacking Indictments and the Frail 'Norm' Against Commercial Espionage," *Lawfare* (blog), November 30, 2017, accessed February 10, 2018, https://lawfareblog.com/chinese-hacking-indictments-and-frail-norm-against-commercial-espionage.

97 Goldsmith and Williams, "The Chinese Hacking Indictments."

98 Goldsmith and Williams, "The Chinese Hacking Indictments."

99 Kenneth Lieberthal and Peter W. Singer, "Cybersecurity and U.S.-China Relations," Brookings Institution, February 2012, 21, accessed February 10, 2018, https://www.brookings.edu/wp-content/uploads/2016/06/0223_cybersecurity_china_us_lieberthal_singer_pdf_english.pdf. See also Michael N. Schmitt and Liis Vihul, "Proxy Wars in Cyberspace: The Evolving International Law of Attribution," *Fletcher Security Review* 1, no. 2 (Spring 2014): 55, 57–67.

100 See, e.g., Samuel J. Rascoff, "The Norm against Economic Espionage for the Benefit of Private Firms: Some Theoretical Reflections," *University of Chicago Law Review* 83 (2016): 249, 250–51.

101 DOJ, "U.S. Charges Five Chinese Military Hackers."

102 White House, "State Visit Fact Sheet"; PRC Ministry of Foreign Affairs, "President Xi's Visit to the United States."

103 "G20 Leaders' Communiqué: Antalya Summit, 15–16 November 2015," Ministry of Foreign Affairs of Japan, accessed February 10, 2018, www.mofa.go.jp/files/000111117.pdf ("We affirm that no country should conduct or support ICT-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").

104 DOJ, "U.S.-China Cybersecurity Dialogue."

105 FireEye, "Red Line Drawn," 14–15; David E. Sanger, "Chinese Curb Cyberattacks on U.S. Interests, Report Finds," *New York Times*, June 20, 2016, accessed February 10, 2018, https://www.nytimes.com/2016/06/21/us/politics/china-us-cyber-spying.html?_r=1; Adam Segal, "The U.S.-China Cyber Espionage Deal One Year Later" (blog), Council on Foreign Relations, September 28, 2016, accessed February 10, 2018, https://www.cfr.org/blog/us-china-cyber-espionage-deal-one-year-later.

106 Cory Bennett, "Why Trump is Sticking with Obama's China Hacking Deal," *Politico*, November 8, 2017, accessed February 10, 2018, https://www.politico.com/story/2017/11/08/trump-obama-china-hacking-deal-244658.

107 Compare Joseph Menn and Jim Finkle, "Chinese Economic Cyber-Espionage Plummets in U.S.: Experts," *Reuters*, June 20, 2016, accessed February 10, 2018, www.reuters.com/article/us-cyber-spying-china-idUSKCN0Z700D, with Doug Olenick, "U.S.-China Cyber Agreement: Flawed, But a Step in the Right Direction," *SC Media*, January 24, 2017, accessed February 10, 2018, https://www.scmagazine.com/us-china-cyber-agreement-flawed-but-a-step-in-the-right-direction/article/633533.

108 US Department of Justice, "U.S. Charges Three Chinese Hackers Who Work at Internet Security Firm for Hacking Three Corporations for Commercial Advantage," news release, November 27, 2017, accessed February 10, 2018, https://www.justice.gov/opa/pr/us-charges-three-chinese-hackers-who-work-internet-security-firm-hacking-three-corporations.

109 U.S. v. Wu Yinzhuo et al., Crim. No. 17-247, 3 (Western District of Pennsylvania, filed September 13, 2017), accessed February 10, 2018, https://www.justice.gov/opa/press-release/file/1013866/download.

110 Insikt Group, "Recorded Future Research Concludes Chinese Ministry of State Security Behind APT3," *Recorded Future* (blog), May 17, 2017, accessed February 10, 2018, https://www.recordedfuture.com/chinese-mss-behind-apt3; "APT3 is Boyusec, a Chinese Intelligence Contractor," *Intrusion Truth*, May 19, 2017, accessed February 10, 2018, https://intrusiontruth.wordpress.com/2017/05/09/apt3-is-boyusec-a-chinese-intelligence-contractor.

111 U.S. v. Wu Yinzhuo, 7.

112 Rascoff, "The Norm against Economic Espionage," 252–53.

113 Donald J. Trump, Twitter, November 10, 2017, 2:43 a.m., accessed February 10, 2018, https://twitter.com/realDonaldTrump/status/928936220360503296.

114 See Kristen E. Eichensehr, "Public-Private Cybersecurity," *Texas Law Review* 95 (2017):467, 470–71.

115 Rascoff, "The Norm against Economic Espionage," 267, 268.

116 James R. Clapper, "Statement by Director of National Intelligence James R. Clapper on Allegations of Economic Espionage," Office of the Director of National Intelligence, September 8, 2013, accessed February 10, 2018, https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2013/item/926-statement-by-director-of-national-intelligence-james-r-clapper-on-allegations-of-economic-espionage.

117 Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge, UK: Cambridge University Press, 2017).

118 "The International Law of Peacetime Cyber Operations—The Hague Launch of the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations and a Panel Discussion," Asser Institute Centre for International & European Law, February 13, 2017, 2, accessed February 10, 2018, www.asser.nl/media/3515/report-the-hague-launch-of-the-tallinn-manual-20-on-the-international-law-applicable-to-cyber-operations.pdf.

119 Schmitt, *Tallinn 2.0*, paragraph 1 of commentary to Rule 33, p. 175.

120 Schmitt, *Tallinn 2.0*, para. 3 of commentary to Rule 33, p. 175.

121 Schmitt, *Tallinn 2.0*, Rules 15 and 17, pp. 87, 94.

122 Schmitt, *Tallinn 2.0*, paras. 1–4 of commentary to Rule 15, pp. 87–88.

123 Schmitt, *Tallinn 2.0*, paras. 4–5 of commentary to Rule 15, p. 88.

124 Schmitt, *Tallinn 2.0*, para. 13 of commentary to Rule 15, p. 91.

125 Schmitt, *Tallinn 2.0*, para. 11 of commentary to Rule 15, p. 90.

126 Schmitt, *Tallinn 2.0*, para. 1 of commentary to Rule 17, p. 95 (quoting art. 8 of the Articles on State Responsibility).

127 See, e.g., Scott J. Shackelford & Richard B. Andres, "State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem," *Georgetown Journal of International Law* 42 (2011): 971; Schmitt & Vihul, "Proxy Wars in Cyberspace," 57–67.

128 Schmitt, *Tallinn 2.0*, paras. 5–6 of commentary to Rule 17, p. 96; Schmitt and Vihul, "Proxy Wars in Cyberspace," 70–72.

129 Schmitt, *Tallinn 2.0*, para. 6 of commentary to Rule 17 (footnotes omitted), p. 96.

130 Schmitt, *Tallinn 2.0*, para. 8 of commentary to Rule 17, p. 97.

131 Schmitt, *Tallinn 2.0*, para. 8 of commentary to Rule 17, p. 97.

132 Schmitt, *Tallinn 2.0*, para. 8 of commentary to Rule 17, p. 97.

133 Milhaupt and Zheng, "Beyond Ownership," 668.

134 Schmitt & Vihul, "Proxy Wars in Cyberspace," 66.

135 Schmitt & Vihul, "Proxy Wars in Cyberspace," 66.

136 Schmitt & Vihul, "Proxy Wars in Cyberspace," 66.

137 UN GGE, Digital Watch Observatory, accessed February 10, 2018, https://dig.watch/processes/ungge.

138 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, section 2, para. 19, accessed February 10, 2018, www.un.org/ga/search/view_doc.asp?symbol=A/68/98&referer=/english/&Lang=E.

139 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, United Nations General Assembly, July 22, 2015, section 6, para. 28(e), accessed February 10, 2018, www.un.org/ga/search/view_doc.asp?symbol=A/70/174.

140 Michael Schmitt and Liis Vihul, "International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms," *Just Security*, June 30, 2017, accessed February 10, 2018, https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms.

141 Michele G. Markoff, "Explanation of Position at the Conclusion of the 2016–2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security," US Department of State, June 23, 2017, accessed February 10, 2018, https://www.state.gov/s/cyberissues/releasesandremarks/272175.htm.

142 *Tallinn 2.0* recognizes a state's sovereign right to restrict access to cyberspace within its territory. See *Tallinn 2.0*, Rules 1, 2 (and accompanying commentary). It asserts that in doing so, a state must take account of international human rights norms, including freedom of expression, but acknowledges that such rights are themselves subject to state limits "that are necessary to achieve a legitimate purpose, non-discriminatory, and authorized by law." *Tallinn 2.0*, Rule 37, pp. 201–2. These include limits on "the enjoyment or exercise of certain human rights in order to protect other rights and to maintain national security and public order, including with respect to activities in cyberspace." *Tallinn 2.0*, para. 1 of commentary to Rule 37, p. 202. Unsurprisingly, the International Group of Experts did not achieve consensus on how to interpret the scope of such national security carve-outs. See *Tallinn 2.0*, Rule 35 (commentary para. 4, p. 188) and Rule 37 (commentary paras. 7–9, pp. 204–5).

143 The head of the Israeli National Cyber Bureau, for example, has argued, "The norm of 'do not attack critical infrastructures' sounds great, but can you define for me what critical infrastructures are? . . . The definition in every nation is different. Some will define everything as critical." Tim Maurer, "UN Body Considers International Cyber Norms," *IHS Jane's Intelligence Review* 53 (December 2016), accessed February 10, 2018, http://carnegieendowment.org/files/F3_Cyber_norms.pdf.

144 Healey, "The Spectrum of National Responsibility for Cyberattacks," 43.

145 DOJ, "U.S.-China Cybersecurity Dialogue."

146 It would be useful to know, for example, to what extent the complicated connections between state and private actors outlined in this paper may factor into the thinking of Chinese analysts and government officials who continue to assert that attribution in the cyber domain is "nearly impossible." See Michael Sulmeyer and Amy Chang, "Three Observations on China's Approach to State Action in Cyberspace," *Lawfare* (blog), January 22, 2017, accessed February 10, 2018, https://www.lawfareblog.com/three-observations-chinas-approach-state-action-cyberspace.

147 Aruna Viswanatha, Robert McMillan, and Nick Timiraos, "U.S. Indicts Three Chinese for Alleged Cyberattacks on Moody's, Siemens," *Wall Street Journal*, November 27, 2017, accessed February 10, 2018, https://www.wsj.com/articles/three-chinese-hackers-indicted-in-u-s-for-alleged-attacks-on-moodys-siemens-1511808500?mg=prod/accounts-wsj.

148 Ellen Nakashima, "Treasury and Justice Officials Pushed for Economic Sanctions on China over Commercial Cybertheft," *Washington Post*, December 27, 2016, accessed February 10, 2018, https://www.washingtonpost.com/world/national-security/2016/12/27/fc93ae12-c925-11e6-8bee-54e800ef2a63_story.html?utm_term=.b2b33afdfb3f.

The preferred citation for this publication is Robert D. Williams, The 'China, Inc.+' Challenge to Cyberspace Norms, Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper No. 1803 (February 22, 2018), available at https://lawfareblog.com/china-inc-challenge-cyberspace-norms.

About the Author

ROBERT D. WILLIAMS

Robert D. Williams is a senior research scholar, lecturer, and executive director of the Paul Tsai China Center at Yale Law School, where he focuses on US-China relations and Chinese law and policy.

Synopsis

This paper explores two aspects of China's governance model that pose distinctive challenges to the construction of international cyberspace norms: the embedded and intertwined nature of the Communist Party-state in China's economy and the expansive conception of national security reflected in Chinese laws and policies. Viewed in conjunction with Chinese cyberspace strategy and activity, these characteristics of "China, Inc. +" raise vexing questions with considerable implications for US-China relations.

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