Pouring 'New' Wine into New Bottles: China-U.S. Deterrence Relations in Cybersace

by Dr. Lora Saalman

Introduction

Within China, pouring "old wine into new bottles" translates into treating the contents of a preexisting concept as if they were new. This phrase applies to how analyses on deterrence in cyberspace continue to echo those on nuclear deterrence.[1] And yet, there are indications that the cyber realm is moving beyond old constructs to a new form of deterrence predicated on greater symmetry and transparency.[2]

Even in a realm in which Chinese analysts lament U.S. hegemony, Beijing's investment in the sciences at an estimated $10.1 billion in 2015 places it in a unique position to close the gap and to articulate its scope, aims, and activities in cyberspace, among any number of other fields. And even where attribution remains a challenge, demonstration of Beijing's and Washington's capabilities in cyberspace shapes incident planning and incident response. Improvements in cyber forensics and China's launch of its Micius quantum communications satellite suggest that "deterrence by detection" and "deterrence by denial" may not be that far off.[3]

In the near term, however, the threat of punishment via coercion is serving as the modus operandi within the China-U.S. cyber deterrence relationship. To date, ironically, this has meant a degree of progress. High-level talks held between Washington and Beijing towards the end of 2015 had their roots in both capitals' practice of this "deterrence by punishment" and growing parallelism in the realization of threats in cyberspace.

Among these, Beijing faced the threat of sanctions and diplomatic fall-out following the indictment of People's Liberation Army (PLA) officers from Unit 61398. Washington confronted the potential for future espionage or blackmail elicited from information allegedly infiltrated by Chinese hackers from the U.S. Office of Personnel Management (OPM). As articulated by analysts in China, the United States only takes a country seriously once it demonstrates capabilities that are of concern.[4]

Conversely, U.S. analysts often point to sanctions as the most viable means to name and shame a country. Nonetheless, questions remain as to

Dr. Lora Saalman *is the Director for the China and Global Security Programme at the Stockholm International Peace Research Institute (SIPRI).*

المنارة للاستشارات

whether these two "deterrence by punishment" trajectories are sustainable and stable within the larger China-U.S. relationship. To better understand this phenomenon, this paper explores Chinese writings and interviews to determine how cyberspace may be replacing old constructs with new ones in China-U.S. deterrence.

Cyber Framework

Much has been written on Washington's use of sanctions and other means to deter behavior. Within Beijing, "deterrence by punishment" is rooted in "information deterrence" (*xinxi weishe*), which has been evolving since the first Iraq war in the early 1990s.[5] Even the concept of "cyber" (*wangluo*) is a relatively new entrant into the Chinese lexicon in which "information" (*xinxi*) is the cornerstone. Within this discourse, information can be used to gain advantage in combat, to exert coercive leverage, or to retaliate. A profusion of Chinese writings has emerged to address the technological means needed to shore up China's cyber defenses, intrusion detection, and response to attacks. These analyses suggest that Beijing is looking to extend its "Great Firewall" into strengthened encryption and cloud networks, quantum communications, and red team exercises. It seeks via these measures to decrease its dependence on external software and hardware supply chains and networks.[6]

In achieving these aims, Chinese writings place a premium on comprehending, countering, and controlling capabilities to garner "major power weapons" (*daguo wuqi*), listing nuclear weapons, anti-satellite systems, and more recently cyber weapons within this pantheon.[7] These new elements fit neatly into Beijing's "Strong Military Dream" (*qiangjun meng*), which in line with the "China Dream" (*zhongguo meng*) advocates mastering the technology needed to build powerful armed forces.[8] Precepts derived from U.S. forces include being first to the fight with information superiority, unified perception, rapid decision-making, self-synchronization, dispersal of forces, and expanded deployment of sensors.[9] While enhanced monitoring capabilities suggest a degree of "deterrence by detection," ultimately the focus in China is on being able to coerce and punish one's adversary for provocative behavior. These writings suggest that such capabilities can be used either preemptively to forestall physical aggression or in retaliation to cyber attacks.

المنارة للاستشارات

Within these Chinese studies, military use of cyberspace is anticipated to bring transparency both on and off the battlefield, increasingly smart weapon platforms, improved target tracking, intelligence-based reconnaissance, electromagnetic countermeasures, jointness, command and control, as well as precision in information management and control of warfighting conditions.[10] As part of building up a strong security environment, malware-based intelligence, reconnaissance, attacks, interruption, and destruction feature prominently into Chinese technical volumes.[11] In essence, the overall goal in these volumes is to achieve military, economic, or political aims without having to send soldiers to the fight.[12]

Among these analyses, members of the Chengdu Military Region Information Office and the Chengdu Military Information Command Department stress the need to master limiting, weakening, severing, destroying, and confusing enemy systems as part of "electromagnetic network attack deterrence."[13] Network-centric espionage and attacks go hand-in-hand, with the latter geared towards system destruction, misinformation, and integrated combat.[14] Thus, much of what is being allegedly exfiltrated from U.S. systems is tailored to provide "deterrence by punishment" via everything from enhanced weapons platforms to personally identifiable information. This suggests that cyber deterrence for China equates with building U.S. concern over punishment or reprisal via not only obtaining the information high ground, but also demonstrating this capability.

This turns the "lack of attribution" argument on its head, since deterrence requires a degree of visibility. Thus, it is not entirely a surprise that forensic reports and penetration tests abound stating that state and non-state Chinese hackers "do not seem to care" about getting caught in acts of espionage, interception, interruption, modification, and fabrication.[15] While some of this transparency occurs due to the profusion of hackers with varying levels of skill-sets, it also serves the purposes of deterrence. In other words, intrusions and attacks that come to light create concerns on the part of the target over how information gleaned and the level of penetration may be used for broader and more coercive activities. Whether intentional or due to inexperience, detection illuminates activities and capabilities that are prerequisites for deterrence in cyberspace. The question is under what conditions and to what ends these attacks occur. Rather than serving as a hindrance to deterrence, incomplete attribution in cyberspace may actually be a corollary to "strategic ambiguity" in the nuclear sphere.

المنارة للاستشارات

Overall, cyber deterrence in China is not linear and is much broader than the nuclear activities and actors contributing to traditional nuclear deterrence. It covers a wide array of both state and non-state entrants within physical, information, perception, and social arenas.[16] According to this holistic framework, cyber warfare has no real beginning or end, given its ties to broader "information operations" (*xinxi xingdong*) and "public opinion warfare" (*yulun zhan*).[17] China's alleged approach of employing academia, industry, foundations, civil government, and military offers a much broader group of actors in cyberspace. Indications are that those with lesser skill-sets serve the function of weakening perimeters, while the more advanced establish command and control once inside the systems. Understanding this range of skills and activities is crucial to parsing how deterrence is operationalized in cyberspace.

*"Cyber warfare has no real beginning or end, given its ties to **[xinxi xingdong]** and **[yulun zhan].**"*

Cyber Activities

Despite the fixation on attribution as a hindrance to cyber deterrence, numerous open source forensic reports dissect Chinese activities in cyberspace.[18] If even a percentage of these cyber intrusions and attacks may be traced back to China, they demonstrate that Beijing's capabilities are accelerating ahead of its posture. While China's 2014 Defense White Paper refers to its military use of cyberspace, this was a belated assessment of a burgeoning field of cyber activities. More than any other sphere, capabilities are not simply driving posture. Instead, Beijing's cyber posture is seemingly unable to keep apace. In light of this disconnect, countless Chinese books and articles dissect U.S. frameworks on regulation, management, exercises, training, and doctrine in cyberspace.[19] Even those purporting to investigate foreign cyber and information warfare from a variety of countries spend the bulk of their time on Washington.[20] These writings suggest that just as much attention is being allocated in Beijing on compromising these structures as on modeling parts of its own cyber apparatus upon them.[21]

Despite indications that Chinese power structures may emulate infrastructure found elsewhere, as with potential establishment of a Cyber Command within China,[22] Beijing has embarked on its own path with a spin-on approach to cyber advances. This contrasts with the U.S. spin-off tradition in which technology and knowledge transfers flow from military

المنارة للاستشارات

to civilian sectors. Reports detail how the Ministry of State Security and the PLA provide grants to universities, industries, and foundations, providing enclaves or segmentation within a much broader network.[23] In an ironic twist, outsourcing is part of the Chinese network. This whole-of-society approach to cyberspace differs from nuclear deterrence in that it posits not simply holding specific targets at risk, but rather the entire interconnected network of civilian and military infrastructure.[24]

This diffuse network can pose difficulties for command and control, yet it also provides greater access to foreign technology and cooperation via civilian industry. The flow of information from civilian to military sectors also allows for part of the network to be sacrificed to save the whole. Therefore, while Chinese analyses bemoan their lack of integration and jointness, this dispersed approach offers advantages to survivability.[25] Recent indications include the criminal proceedings in China tied to the hacking of OPM and to the industrial espionage incidents compromising Westinghouse, SolarWorld, U.S. Steel, Allegheny Technologies, and Alcoa. In these cases, Chinese authorities have purportedly made a few targeted arrests of individuals, but these are likely to have only superficially addressed the larger network within China.

In spite of these flashpoints, Chinese writings and actions suggest an ever-growing appreciation for many of the same concerns faced by the United States, from lagging domestic and international legal frameworks to exfiltration of information through backdoors into computer systems.[26] Cyber threats from theft of data, tampering and destruction of software and hardware, attacks against critical infrastructure, installation of backdoors within supply chains, disabling of weapon systems, enabling of kinetic attacks from near space vehicles, and lack of adequately trained cyber recruits in military and government are common themes throughout Chinese analyses.[27] These concerns belie the fact that Beijing's main threat perception comes from Washington, both in terms of cyber attacks and cyber norms.[28]

U.S. reports on China are also rife with concerns, suggesting that—even in the face of incomplete attribution—both countries are shaping their response on perception, as much as experience. Experts within the Electronic Countermeasures Center in China lament that U.S.-driven legal mechanisms and norms may constrain China's own offensive cyber warfare, electronic warfare, electromagnetic warfare, and psychological warfare

المنارة للاستشارات

developments.[29] Chinese strategists further highlight how Western interests could adversely impact Beijing's ability to develop countermeasures against radars and telecommunications, as well as interfere with land-based satellite telecommunications and global positioning systems.[30] This connectivity echoes U.S. writings on China's own potential disabling or destruction of U.S. weapons systems, guidance, and critical infrastructure. Despite the overlap among these points of concern, the fact that Beijing and Washington lack mechanisms for arms control and verification in cyberspace complicate meaningful exchange between the two on cyber deterrence.[31]

Cyber Deterrence

The relative lack of a bilateral discourse on cyber deterrence does not mean that writings on the topic are lacking in China. In fact, one of the more striking aspects of Chinese writings on cyber deterrence is that much of the terminology is similar to that found within those on nuclear deterrence. Notable examples include references in both arenas to perceived U.S. "absolute security" (*juedui anquan*), "absolute superiority" (*juedui youshi*), and role as a "hegemon" (*bazhu*).[32] In contrast to nuclear deterrence, however, U.S. dominance in cyberspace is not as apparent. This could be why some Western analysts have observed that Chinese experts do not rank cyberspace as that high of a concern when discussing the state of China-U.S. relations.[33] The asymmetry is not as pronounced.

As cyber security plays an ever-increasing role in such critical infrastructure as nuclear facilities, arsenals, delivery systems, and command and control centers, the conceptual chasm separating cyber deterrence and nuclear deterrence is likely to further diminish, along with historical China-U.S. asymmetry.[34] From an arms control perspective, this opens up new avenues to explore the pronounced differences between nuclear deterrence and cyber deterrence, as in the chart below.[35]

China on Nuclear Deterrence	China on Cyber Deterrence
Transparency of Intent Over Capabilities	Transparency of Capabilities Over Intent
Not Preemptive, Guided by No First Use	Preemptive and Retaliatory, Lack of Set Doctrine
Minimum Nuclear Deterrence Sets Boundaries	Not Constrained by Scope or Boundaries
Select Actors: Party, Government, Second Artillery/Rocket Force	Diffuse Actors: PLA, MSS, Academia, Industry, Foundations, Individuals
Has Mechanisms for Verification	Lacks Mechanisms for Verification
Attribution Strong	Attribution Limited
Sizeable Asymmetry with the United States	Growing Symmetry with the United States

للاستشارات

Beyond theory, the practical application of cyber deterrence has yet to reach the impasse found in China-U.S. nuclear engagement that emerged with the release of the Report of the Select Committee on U.S. National Security and Military/Commercial Concerns with the People's Republic of China, more commonly known as the Cox Report. This official document, issued in the late 1990s, alleged Chinese theft of nuclear warhead designs. In doing so, it scuttled much of the official and scientific China-U.S. nuclear exchange into present day.

By contrast, despite the current prevailing narrative that the PLA indictments have stymied high-level China-U.S. talks on cyberspace, it took only a year from the cessation of cyber talks for them to reemerge.[36] In fact, these China-U.S. talks have become more regularized and more specific in the wake of both the PLA indictments and OPM hack, reaching a higher rank of participants, expanding tabletop exercises, and establishing a hotline.[37] In effect, these talks have created a road map for guidelines in combatting cyber-crime. The speed with which Washington and Beijing came back to the negotiating table suggests an ability in cyberspace to move beyond the seemingly intractable nuclear strategic stability paradigm.

When it comes to strategic stability, the vast China-U.S. asymmetry in the nuclear realm does not exist to the same degree in cyberspace. Diminished asymmetry, however, does not mean that it is non-existent. Chinese analyses continue to highlight the need for Beijing's own advances in strengthening of information warfare theory, establishment of military private networks, construction of information platform management and application of core technologies, as well as standardization of the internet of things, cyber security, and information security.[38] In terms of overall capabilities, despite such Chinese experts as General Zhang Chaozhong noting the difficulty of cyber attacks on networks, data storage, and nuclear control codes of the U.S. Department of Defense, any number of hacking incidents illustrate China's vast and varied approach has yielded results far beyond alleged hacks related to the PLA or against OPM.[39]

For the United States, rather than despairing over this erosion of asymmetry, the shift from China's transparency of intent to transparency of capabilities in cyberspace may offer the potential for a stronger basis for engagement than in the nuclear arena. Rather than being relegated to debating a set of actions that China might or might not undertake, there is enough information readily available within open source forensics reports

المنارة للاستشارات

to enhance understanding of capabilities, characteristics, patterns, and signatures of cyber intrusion and attack. Understanding these activities is critical to advancing cyber deterrence in terms of incident planning and incident response. It also offers a chance to move beyond "strategic ambiguity." Thus, while much of available research focuses on forensics targeting individual hacking cases, more time needs to be spent connecting various campaigns and signatures together for a more systematic and synthesized approach.

As one example, depending upon the forensic report, Deep Panda, Axiom, Group 72, Shell Crew, Elderwood, and Black Vine have all been linked to either preparation for or execution of the OPM hack. Diversity of reporting and threat actor labels is not likely confined to just the cyber security industry, but also to the range U.S. government offices and departments still vying for their own authority on cyberspace issues. Sorting among these various organs and cases to find connectivity among disparate hacks is essential for moving beyond isolated signatures towards broader networks. Recent China-U.S. talks addressed a degree of this plurality within China's domestic cyber network in that they engaged the Central Political and Legal Affairs Commission of the Chinese Communist Party, Ministry of Public Security, China's Ministry of State Security, Ministry of Justice, and the State Internet and Information Office. Yet, this still leaves any number of other organizations with vested interests and roles in cyber deterrence out of the conversation.

"Understanding these activities is critical to advancing cyber detterence in terms of incident planning and incident response."

Among these, the Cyberspace Administration of China, which falls under both the Chinese government and to the Chinese Communist Party, serves as an umbrella organization that is working on playing a formative role when it comes to the Internet, overseeing each of column of Chinese cyber activities from civil to military. Another organization for future engagement is likely to follow with the establishment of a Cyber Command in China.[40] Greater consolidation of Chinese cyber strategy and operationalization would not necessarily run counter to U.S. interests. Rather, it would provide channels of interlocutors within similar structures for future China-U.S. exchanges on cyber deterrence. Having the U.S. Department of Homeland

المنارة للاستشارات

Security and Cyber Command as counterparts to such organizations in China would provide a greater degree of predictability and the potential for engagement on escalation management, mitigation of strategic ambiguity, and setting of norms in cyberspace.

Conclusion

The more that China and the United States resemble each other in cyberspace in both capabilities and concerns, the greater the chance that the two will be able to move beyond the asymmetry dilemma that currently confounds sustained high-level engagement on strategic stability and nuclear deterrence. This is not to say that their advances in cyberspace are entirely in sync or will be wholly stabilizing. China's current diffuse set of actors that include academia, industry, foundations, civilian government, and military suggest that it is developing an asymmetrical advantage in scale and scope of effort. As much as China has taken on some U.S. attributes in cyberspace, Washington may find itself compelled to become more like Beijing with a wider array of entrants into the field. The debate in the United States over whether private industry should undertake a greater role in active defense and hacking back in the wake of the cyber attack on Sony Pictures is just one manifestation of this potential expansion. Both countries' pursuits in forensics, countermeasures and quantum communications draw them ever closer and perhaps one day towards more sustainable norms and long-term stability under "deterrence by detection" and "deterrence by denial."

Currently, however, the China-U.S. trend towards "deterrence by punishment" as the predominant form of cyber deterrence suggests the potential for increasing brinksmanship. While this might bring both sides to the negotiation table in the short-term, it lacks the nuance needed to confront the cyber intrusions and attacks that both countries will face in the long-term. The threat of punishment or coercion will remain ever-present to respond to larger-scale or more severe incidents. Yet, an expanded commitment in China to shore up its domestic defense-in-depth and in Washington to extend its cyber security "sprint" to a marathon would provide a more sustainable foundation for cyber deterrence predicated on strengthening weak detection and denial capabilities in both countries. By pouring "new" wine into new bottles, China-U.S. cyber deterrence could avoid some of the pitfalls of escalation found in nuclear deterrence, providing a more workable model for future strategic stability.

المنارة للاستشارات

Notes

[1] While these writings seek to debunk the use of nuclear frameworks to analyze deterrence in cyberspace, they nonetheless still make frequent reference to and use a basic construct found in nuclear deterrence calculations. A few of the more recent iterations include Joseph S. Nye, "Can Cyber Warfare Be Deterred?" *Project Syndicate*, December 10, 2015, available at https://www.project-syndicate.org/commentary/cyber-warfare-deterrence-by-joseph-s--nye-2015-12; Scott Warren Harold, Martin C. Libicki, and Astrid Stuth Cevallos, "Getting to Yes with China in Cyberspace," *RAND Corporation*, 2016, available at http://www.rand.org/content/dam/rand/pubs/research_reports/RR1300/RR1335/RAND_RR1335.pdf.

[2] Based on discussions held by the author with Chinese experts in Beijing, China in 2014, 2015, and 2016 at the China Institutes of Contemporary International Relations, China Institute of International Studies, Chinese Academy of Social Sciences, the University of International Business and Economics, as well as Tsinghua University's 2016 Annual Conference of the Chinese Community of Political Science and International Studies.

[3] Josh Chin, "China's Latest Leap Forward Isn't Just Great—It's Quantum," *The Wall Street Journal*, August 20, 2016, available at http://www.wsj.com/articles/chinas-latest-leap-forward-isnt-just-greatits-quantum-1471269555.

[4] Based on doctoral dissertation research and interviews conducted by the author in Beijing and Shanghai from 2006-2010, while at Tsinghua University.

[5] Tang Yueping, Zhao Weifeng, Yu Maizheng, Sun Jian, Han Ping, and Tang Shaoqing, *Keji xinxi yun fuwu ji junshi yingyong* [*Science and Technology Information of (sic.) Cloud Services and (sic.) Military Application*], (Beijing: National Defense Industry Press, 2015), pp. 257-258.

[6] Song Hang, *Hulianwang jishu ji qi junshi yingyong* [In*ternet of Things Technology and Its Military Use*], (Beijing: National Defense Industry Press, 2015), p. 168-170; Tang Yueping, Zhao Weifeng, Yu Maizheng, Sun Jian, Han Ping, and Tang Shaoqing, *Keji xinxi yun fuwu ji junshi yingyong* [*Science and Technology Information of (sic.) Cloud Services and (sic.) Military Application*], (Beijing: National Defense Industry Press, 2015), p. 273; Song Zhongping, *Daguo wuqi* [*Major Power Weapons*], (Beijing: New World Press, 2013); Song Hang, *Hulianwang jishu ji qi junshi yingyong* [In*ternet of Things Technology and Its Military Use*], (Beijing: National Defense Industry Press, 2015), p. 144; Mao Nanzhang and Zhao Chaonan, "Xinxihua tiaozhanxia wangluo dianci kongjian anquan wenti yanjiu" [Network Electromagnetic Space Security Under Informationized Conditions], In Ji Sanping and Zeng Fengyang, *Jundui xinxihua yu junshi fazhi jianshe* [*Military Informationization and Military Legal Construction*] (Beijing: Military Sciences Press, 2012), pp. 297-303.

[7] Lora Saalman, "Prompt Global Strike: China and the Spear," Asia-Pacific Center for Security Studies, April 2014, available at http://apcss.org/wp-content/uploads/2014/04/APCSS_Saalman_PGS_China_Apr2014.pdf; Lora Saalman, "The China Factor" in Alexei Arbatov and Vladimir Dvorkin, Eds., *Missile Defense: Confrontation and Cooperation*, Carnegie Moscow Center, 2013, available at http://carnegieendowment.org/files/Missile_Defense_book_eng_fin2013.pdf; Lora Saalman, "China and the U.S. Nuclear Posture Review," Carnegie Endowment for International Peace, February 2011, available at http://carnegieendowment.org/2011/02/28/china-and-u.s.-nuclear-posture-review; Song Zhongping, *Daguo wuqi* [*Major Power Weapons*], (Beijing: New World Press, 2013); Song Hang, *Hulianwang jishu ji qi junshi yingyong* [In*ternet of Things Technology and Its Military Use*], (Beijing: National Defense Industry Press, 2015), p. 172; Tao Hongxing and Wen Bohua, *Meijun wangluozhan yanjiu* [*Investigation on (sic.) U.S. Armed Forces Cyber War (sic.)*], (Beijing: National Defense University Publishers, 2010); Lin Pingzhong, Zhou Jun, and Ge Min, *Junshi xinxi guanlixue gailun* [*Prospectus on Military Information Management Studies*], (Beijing: World Publishing Company, 2015), p. 312-329.

[8] Liu Ruojie and Zhang Mengchuan, *Qiang Jun Meng* [*Strong Military Dream*], (Beijing: Academy of Military Sciences Press, 2014).

[9] Liang Yan, *Wangluo zhongxinzhan de shishi yu yingyong fenxi* [R*eality and Utility of Network Centric Warfare*], (Beijing: National Defense Industry Press, 2011), pp. 2-3.

المنارة للاستشارات

[10] Ma Liangli, Wu Qingzhi, Su Kai, and Ren Wei, *Hulianwang ji qi junshi yingyong* [*The Internet of Things and Its Military Applications*], (Beijing: National Defense Industry Press, 2015), p. 187; Song Hang, *Hulianwang jishu ji qi junshi yingyong* [Internet of Things Technology and Its Military Applications], (Beijing: National Defense Industry Press, 2015), p. 168; Zheng Ruobing, *Junshi xinxi anquan lun* [*Military Information Security Theory*], (Beijing: National Defense University Press, 2013), p. 101; Tang Yueping, Zhao Weifeng, Yu Maizheng, Sun Jian, Han Ping, and Tang Shaoqing, *Keji xinxi yun fuwu ji junshi yingyong* [*Science and Technology Information of (sic.) Cloud Services and (sic.) Military Application*], (Beijing: National Defense Industry Press, 2015), p. 258; Song Zhongping, *Daguo wuqi* [*Major Power Weapons*], (Beijing: New World Press, 2013); Song Hang, *Hulianwang jishu ji qi junshi yingyong* [*Internet of Things Technology and Its Military Use*], (Beijing: National Defense Industry Press, 2015), p. 140.

[11] He Mingli, Fan Xingquan, and Liu Gangfeng, *Junyong wuxian chuanganqi wangluo sheji* [*Military Wireless Sensor Network Design*], (Beijing: National Defense Industry Press, 2015), p. 11.

[12] Ma Nanzhang is Chief Engineer within the Chengdu Military Region Informationization Office and Zhao Chaonan is Deputy Minister within the Chengdu Military Informationization Command Department. Ma Nanzhang and Zhao Chaonan, "Xinxihua tiaozhanxia wangluo dianci kongjian anquan wenti yanjiu" [Network Electromagnetic Space Security Under Informationized Conditions], In Ji Sanping and Zeng Fengyang, *Jundui xinxihua yu junshi fazhi jianshe* [*Military Informationization and Military Legal Construction*], (Beijing: Military Sciences Press 2012), p. 300.

[13] Ma Nanzhang and Zhao Chaonan, "Xinxihua tiaozhanxia wangluo dianci kongjian anquan wenti yanjiu" [Network Electromagnetic Space Security Under Informationized Conditions], In Ji Sanping and Zeng Fengyang, *Jundui xinxihua yu junshi fazhi jianshe* [*Military Informationization and Military Legal Construction*], (Beijing: Military Sciences Press, 2012), p. 300.

[14] Liang Yan, *Wangluo zhongxinzhan de shishi yu yingyong fenxi* [Reality and Utility of Network Centric Warfare], (Beijing: National Defense Industry Press, 2011), p. 210.

[15] "APT1: Exposing One of China's Cyber Espionage Units," Mandiant, 2014, available at http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf; APT30 and the Mechanics of a Long-Running Cyber Espionage Operation," FireEye, April 2015, available at https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf; Arik Hesseldahl, "FireEye Identifies Chinese Group Behind Federal Hack," Recode, June 2015, http://recode.net/2015/06/19/fireeye-identifies-chinese-group-behind-federal-hack.; Lion Gu, "Prototype Nation: The Chinese Cybercriminal Underground in 2015," TrendMicro, 2015, available at https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-prototype-nation.pdf; Wu Yannan, Yang Rennong, Chu Wei, and Wang Xuefeng, *Wangluo jishu ji qi junshi yingyong* [*Cyber Technology and Its Military Application*], (Beijing: National Defense Industry Press, 2014), p. 39.

[16] Liang Yan, *Wangluo zhongxinzhan de shishi yu yingyong fenxi* [Reality and Utility of Network Centric Warfare], (Beijing: National Defense Industry Press, 2011), p. 3.

[17] Song Zhongping, *Daguo wuqi* [*Major Power Weapons*], (Beijing: New World Press, 2013); Song Hang, *Hulianwang jishu ji qi junshi yingyong* [*Internet of Things Technology and Its Military Use*], (Beijing: National Defense Industry Press, 2015), p. 140. Zhou Hao is the Deputy Director of the Electronic Countermeasure Center. Li Bo and Wang Lu are experts at the Electronic Countermeasure Center. Zhou Hao, Li Bo, and Wang Lu, "Wangluo dianci kongjian zuozhan sheji guojifa wenti yanjiu yu sikao" [Study and Reflection on Legal Issues Raised by Network Electromagnetic Space Warfare], In Ji Sanping and Zeng Fengyang, *Jundui xinxihua yu junshi fazhi jianshe* [*Military Informationization and Military Legal Construction*], (Beijing: Military Sciences Press, 2012), p. 127.

[18] "APT1: Exposing One of China's Cyber Espionage Units," Mandiant, 2014, available at http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf; APT30 and the Mechanics of a Long-Running Cyber Espionage Operation," FireEye, April 2015, available at https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf; Arik Hesseldahl, "FireEye Identifies Chinese Group Behind Federal

المنارة للاستشارات

Hack," Recode, June 2015, http://recode.net/2015/06/19/fireeye-identifies-chinese-group-behind-federal-hack.; Lion Gu, "Prototype Nation: The Chinese Cybercriminal Underground in 2015," TrendMicro, 2015, available at https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-prototype-nation.pdf.

[19] Song Zhongping, *Daguo wuqi* [*Major Power Weapons*], (Beijing: New World Press: 2013); Song Hang, *Hulianwang jishu ji qi junshi yingyong* [*Internet of Things Technology and Its Military Use*], (Beijing: National Defense Industry Press, 2015), p. 142.

[20] Lin Pingzhong, Zhou Jun, and Ge Min, *Junshi xinxi guanlixue gailun* [*Prospectus on Military Information Management Studies*], (Beijing: World Publishing Company, 2015), pp. 312-329.

[21] Wang Guoliang and Luo Zhiyong, *Xinxi wangluo anquan ceshi yu pinggu* [*Examination and Evaluation of Information and Cyber Security*], (Beijing: National Defense Industry Press, 2015), pp. 5, 8-9.

[22] Based on discussions in Beijing, China with a series of cyber experts in October 2014 and December 2015; Song Zhongping, *Daguo wuqi* [*Major Power Weapons*], (Beijing: New World Press, 2013); Song Hang, *Hulianwang jishu ji qi junshi yingyong* [Int*ernet of Things Technology and Its Military Use*], (Beijing: National Defense Industry Press, 2015), p. 145.

[23] For more information, please see Bryan Krekel, Patton Adams, and George Bakos, "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage," Northrop Grumman, Prepared for the U.S.-China Economic and Security Review Commission, March 2012, available at http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-066.pdf.

[24] Tang Yueping, Zhao Weifeng, Yu Maizheng, Sun Jian, Han Ping, and Tang Shaoqing, *Keji xinxi yun fuwu ji junshi yingyong* [*Science and Technology Information of (sic.) Cloud Services and (sic.) Military Application*], (Beijing: National Defense Industry Press, 2015), p. 258.

[25] Tang Yueping, Zhao Weifeng, Yu Maizheng, Sun Jian, Han Ping, and Tang Shaoqing, *Keji xinxi yun fuwu ji junshi yingyong* [*Science and Technology Information of (sic.) Cloud Services and (sic.) Military Application*], (Beijing: National Defense Industry Press, 2015), p. 260.

[26] Chen Xiang, *Mianxiang xinxi fuwu de xinxi jishu* [*Facing Information Technology of Information Services*], (Beijing: National Defense Industry Press, 2013), pp. 34-35, 307-308.

[27] Xu Longdi and Teng Jianqun, "Wangluo junbei ji qi kongzhi: Xin gainian, xin qushi, xin shiming," [Cyber Armaments and Their Control: New Concepts, New Trends, New Mission], in Zhongguo junkong yu caijun xiehui [China Arms Control and Disarmament Association], *Guoji junbei kongzhi yu caijun* [*International Arms Control and Disarmament*], (Beijing: World Knowledge Publishers, 2014), p. 91; Cheng Yimin, "Zhongmei junshi xinxi anquan falv zhidu bijiao yanjiu" [Research on Comparing China-U.S. Military Information Security Laws], In Ji Sanping and Zeng Fengyang, *Jundui xinxihua yu junshi fazhi jianshe* [*Military Informationization and Military Legal Construction*], (Beijing: Military Sciences Press, 2012), pp. 333-334; Song Zhongping, *Daguo wuqi* [*Major Power Weapons*], (Beijing: New World Press, 2013); Song Hang, *Hulianwang jishu ji qi junshi yingyong* [*Internet of Things Technology and Its Military Use*], (Beijing: National Defense Industry Press, 2015), p. 142.

[28] Based on discussions held by the author with Chinese experts in Beijing, China in 2014, 2015, and 2016 at the China Institutes of Contemporary International Relations, China Institute of International Studies, Chinese Academy of Social Sciences, the University of International Business and Economics, as well as Tsinghua University's 2016 Annual Conference of the Chinese Community of Political Science and International Studies.

[29] Zhou Hao is the Deputy Director of the Electronic Countermeasure Center. Li Bo and Wang Lu are experts at the Electronic Countermeasure Center. Zhou Hao, Li Bo, and Wang Lu, "Wangluo dianci kongjian zuozhan sheji guojifa wenti yanjiu yu sikao" [Study and Reflection on Legal Issues Raised by Network Electromagnetic Space Warfare], In Ji Sanping and Zeng Fengyang, *Jundui xinxihua yu junshi fazhi jianshe* [*Military Informationization and Military Legal Establishment*], (Beijing: Military Sciences Press, 2012), pp. 124-127.

المنارة للاستشارات

[30] Zhou Hao, Li Bo, and Wang Lu, "Wangluo dianci kongjian zuozhan sheji guojifa wenti yanjiu yu sikao" [Study and Reflection on Legal Issues Raised by Network Electromagnetic Space Warfare], In Ji Sanping and Zeng Fengyang, *Jundui xinxihua yu junshi fazhi jianshe* [*Military Informationization and Military Legal Establishment*], (Beijing: Military Sciences Press, 2012), pp. 124-127.
[31] Xu Longdi and Teng Jianqun, "Wangluo junbei ji qi kongzhi: Xin gainian, xin qushi, xin shiming," [Cyber Armaments and Their Control: New Concepts, New Trends, New Mission], in Zhongguo junkong yu caijun xiehui [China Arms Control and Disarmament Association], *Guoji junbei kongzhi yu caijun* [*International Arms Control and Disarmament*], (Beijing: World Knowledge Publishers, 2014), p. 93.
[32] Song Hang, *Hulianwang jishu ji qi junshi yingyong* [*Internet of Things Technology and Its Military Use*], (Beijing: National Defense Industry Press, 2015), p. 167; General Chen Zhou is Director of the Academy of Military Sciences. Chen Zhou, *Junshi touminglun* [*The Theory of Military Transparency*], (People's Liberation Army Press, 2013), p. 209.
[33] Scott Warren Harold, Martin C. Libicki, and Astrid Stuth Cevallos, "Getting to Yes with China in Cyberspace," RAND Corporation, 2016, available at http://www.rand.org/content/dam/rand/pubs/research_reports/RR1300/RR1335/RAND_RR1335.pdf.
[34] Securing China's Second Artillery/Rocket Force and nuclear command and control centers from cyber intrusion and attack, combined with training on information technology features into some of the Chinese studies surveyed. Zhou Hao is the Deputy Director of the Electronic Countermeasure Center. Li Bo and Wang Lu are experts at the Electronic Countermeasure Center. Zhou Hao, Li Bo, and Wang Lu, "Wangluo dianci kongjian zuozhan sheji guojifa wenti yanjiu yu sikao" [Study and Reflection on Legal Issues Raised by Network Electromagnetic Space Warfare], In Ji Sanping and Zeng Fengyang, *Jundui xinxihua yu junshi fazhi jianshe* [*Military Informationization and Military Legal Construction*], (Beijing: Military Sciences Press, 2012), p. 229.
[35] Dr. Xu Longdi is an expert working on cyber affairs and Captain (Ret) Dr. Teng Jianqun is Director of the Department for American Studies and a senior research fellow at the China Institute of International Studies, which is affiliated with China's Ministry of Foreign Affairs. Xu Longdi and Teng Jianqun, "Wangluo junbei ji qi kongzhi: Xin gainian, xin qushi, xin shiming," [Cyber Armaments and Their Control: New Concepts, New Trends, New Mission], in Zhongguo junkong yu caijun xiehui [China Arms Control and Disarmament Association], *Guoji junbei kongzhi yu caijun* [*International Arms Control and Disarmament*], (Beijing: World Knowledge Publishers, 2014), pp. 89-106.
[36] Based on discussions held by the author with Chinese experts in Beijing, China in 2014, 2015, and 2016 at the China Institutes of Contemporary International Relations, China Institute of International Studies, Chinese Academy of Social Sciences, the University of International Business and Economics, as well as Tsinghua University's 2016 Annual Conference of the Chinese Community of Political Science and International Studies.
[37] "First U.S.-China High-Level Joint Dialogue On Cybercrime And Related Issues Summary Of Outcomes," Department of Homeland Security, December 2, 2015, available at https://www.dhs.gov/news/2015/12/02/first-us-china-high-level-joint-dialogue-cybercrime-and-related-issues-summary.
[38] Ma Liangli, Wu Qingzhi, Su Kai, and Ren Wei, *Hulianwang ji qi junshi yingyong* [*The Internet of Things and Its Military Applications*], (Beijing: National Defense Industry Press, 2015), p. 187
[39] Song Zhongping, *Daguo wuqi* [*Major Power Weapons*], (Beijing: New World Press, 2013); Song Hang, *Hulianwang jishu ji qi junshi yingyong* [*Internet of Things Technology and Its Military Use*], (Beijing: National Defense Industry Press, 2015), p. 143.
[40] Based on discussions held by the author with Chinese experts in Beijing, China in 2014, 2015, and 2016 at the China Institutes of Contemporary International Relations, China Institute of International Studies, Chinese Academy of Social Sciences, the University of International Business and Economics, as well as Tsinghua University's 2016 Annual Conference of the Chinese Community of Political Science and International Studies.

المنارة للاستشارات

Reproduced with permission of copyright owner. Further reproduction prohibited without permission.

المنارة للاستشارات