Rethinking China-Russia-U.S. Deterrence in Cyber Space

When it comes to cyber deterrence, its nature and very existence come under debate. This essay seeks to challenge key assumptions tied to cyber deterrence and to provide a framework for how it is evolving among China, Russia and the U.S.
Rethinking China-Russia-U.S. Deterrence in Cyberspace

Dr. Lora Saalman, Director and Senior Researcher, China and Global Security Programme, Stockholm International Peace Research Institute (SIPRI)

The nature and very existence of cyber deterrence remain under debate. This ThinkChina.dk policy brief seeks to challenge key assumptions tied to cyber deterrence and to provide a framework for how it is evolving among China, Russia, and the United States. While incidents occurring in the nuclear domain indicate the inherent difficulty of these three countries engaging in meaningful official exchange on mutual vulnerability and strategic stability, cyberspace offers underappreciated levels of transparency and symmetry. These elements of strategic stability may not just be present in cyberspace, but may also offer a foundation for future exchanges. In doing so, setting up the basic groundwork of Chinese, Russian, and U.S. terminology, technology, and targeting represents an essential first step for better understanding how cyber deterrence operates.
Rethinking China-Russia-U.S. Deterrence in Cyberspace

Dr. Lora Saalman, Director and Senior Researcher, China and Global Security Programme, SIPRI

Introduction

China’s People’s Liberation Army Rocket Force, Russia’s Strategic Rocket Force, and U.S. Strategic Command have lengthy traditions of operationalizing nuclear deterrence. Yet, the nature and very existence of cyber deterrence remain under debate. At its most basic level, deterrence is predicated upon convincing an opponent not to engage in a specific action, due to the costs outweighing the benefits of such behavior. Analysis on how other countries perceive this trade-off requires a more nuanced evaluation of each nation’s cyberspace calculations and definitions. To this end, this essay seeks to challenge key assumptions tied to cyber deterrence and to provide a framework for how it is evolving among China, Russia, and the United States.

Transparency and Symmetry

Transparency and symmetry play a much greater role than is often assumed in China-Russia-U.S. cyber relations. On transparency, while lacking the concreteness of nuclear platforms, countries are engaged in activities that demonstrate their cyber capabilities for deterrent or other effect. Whether measured by cost, scale, complexity, or forensic signatures, attribution in cyberspace is growing. To deter an adversary, one must also be able to demonstrate prowess. As just one example, alleged North Korean cyber theft of data and plans for U.S. and South Korean military operations complicates the latter’s use of force in cyberspace and kinetic options. In this case, even incomplete attribution serves North Korean national interests and undermines its adversary’s confidence in engaging in a pre-emptive strike. This undermines the idea that transparency is absent from cyberspace. Attribution, or discovery, can be an advantage when deterring one’s adversary.

On symmetry, readily available malware and hacking tactics have allowed a range of countries to leverage cyber vulnerabilities of adversaries that are stronger in conventional and nuclear systems. This levelling of the playing field confounds traditional calculations of military dominance, by turning digital strength and reliance into a weakness. These trends undermine the argument that any country can truly possess ‘cyber superiority’ (网络优势). In fact, overdependence on cyberspace can be detrimental, exposing a greater threat surface for one’s opponent to leverage and attack. Even countries at an asymmetrical disadvantage like North Korea have demonstrated cyber capabilities that indicate much greater prowess than might otherwise be assumed. Much like guerrilla warfare, they have an enhanced ability to conduct operations that exploit the broader threat surface of their adversary.


3 Whether through access to such tools, techniques, and services through ToR or via such mass exfiltrations as with the Shadow Brokers’ cyber operations against the U.S. National Security Agency, the idea that any one country has an unassailable monopoly on these capabilities is not tenable. Leonhard, Woody, ‘More Shadow Brokers fallout: DoublePulsar zero-day infects scores of Windows PCs’, Computerworld, 24 Apr. 2017, https://www.computerworld.com/article/3191897/microsoft-windows/more…rs-fallout-doublepulsar-zero-day-infects-scores-of-windows-pcs.html.


These challenges to traditional concepts of transparency and symmetry in deterrence merit attention for their impact on China-Russia-U.S. relations. Chinese interlocutors have for decades cited their asymmetrical weakness and resultant inability to be transparent as justifications for why Beijing has been unwilling to engage in track-one level nuclear talks with Moscow and Washington. While this argument may have grounds in the nuclear sphere, it is less convincing in cyberspace. Whether intentional or not, the level of China’s transparency has grown with the volume and signatures of cyber incidents emanating from its territory. Moreover, China’s rapid and comprehensive acquisition of cyber capabilities makes it harder to argue that it remains at a categorical disadvantage vis-à-vis Russia and the United States.

Beyond transparency and symmetry, Beijing’s conceptual gap with Moscow and Washington on cyberspace is also eroding. A survey of 400 Chinese-language writings finds that 56 percent of those surveyed utilize the Russian construct of ‘information deterrence’ (信息威慑) and the U.S.-centric term ‘cyber deterrence’ (网络威慑). Chinese experts apply ‘information deterrence’ to the Ukraine conflict, as well as to employment of Russian electronic disruption and information warfare. Their coverage of Russian activities posits a holistic approach towards cyberspace that seeks to leverage and to control information flows. Further, China’s domestic structure mirrors this approach with its own much-touted national firewall, emphasis on cyber sovereignty under the Cyberspace Administration of China, as well as alleged APT30 operations in Southeast Asia to monitor and to potentially influence local government, industry, and media.9

When it comes to the United States, Chinese analysts apply the term ‘cyber deterrence’ to characterize advances that underpin U.S. nuclear modernization and third offset strategy.10 Cyber operations are seen as vehicles for bolstering U.S. conventional and nuclear platforms and in undermining the systems of other countries.11 To counter this

---

2 Ling Shengyin and Chen Wang are affiliated with the Army Political Department of the Nanjing Army Command College. 凌胜银 and 陈旺 are affiliated with the Army Political Department of the Nanjing Army Command College.
5 马建光 (Ma Jianguang) and 张乃千 (Zhang Naqian), ‘美俄网络对峙，俄罗斯准备好了吗?’ (U.S.-Russia Cyber Confrontation, Is Russia Ready?), 科技日报 (Science and Technology Daily), 31 Aug. 2016, p. 6; 李大光 (Li Daguang), ‘第三次抵消战略保持美军优势的关键技术’ (The Third Offset’ Maintaining U.S. Military Advantage in Key Technologies), 国际视野 (International Observer), pp. 77-79.
threat, a range of Chinese publications discuss the importance of hardening datalinks, while undermining systems connected to U.S. hypersonic glide, missile defense, and other platforms.12 Thus, while official documents on cyberspace still lean towards the framework found in the codes of conduct submitted to the United Nations General Assembly in 2011 and 2015,13 Chinese academic, technical, and military communities place Beijing at various points along a spectrum between Moscow-centric ‘information deterrence’ and Washington-centric ‘cyber deterrence’.14

Despite the seeming chasm between Russian and U.S. views on cyberspace, China is not alone in shifting its position along this arc.

Washington and Moscow are also growing in similarity. Alleged Russian reconnaissance aimed at future cyber-attacks against critical infrastructure, and already thought to have been employed in Ukraine and Georgia, indicates the capability of drawing a sharp line between information and kinetic cyber operations.15 Further, the mass exfiltration of data from U.S. government and other facilities has also led to a redefinition in Washington of information theft and manipulation as attacks on critical infrastructure. As Russia and the United States are pulled toward the center in defining the nuances of information versus cyber operations and deterrence in cyberspace, they are likely to meet in the middle with China.16

**Defensive, Detection, and Punishment Deterrence**

When it comes to deterrence in cyberspace, one of the most commonly applied theoretical constructs is ‘deterrence by denial’ that assumes ‘the capability to deny the other party any gains from the move which is to be...

---


16 Thus, while all three countries may still differ on what constitutes a cyber weapon and whether it could be deemed to be a weapon of mass destruction, there is relative consensus that it can be used as a weapon of mass disruption. Much of this relates to the nature of the target. Accordingly, the United Nations Governmental Group of Experts (UNGGIE) has largely centered its growing consensus on identifying the legality of what is being attacked. Conditions on the ground have also ushered this shift, as with the recent two cases of cyber attacks on the operation of Ukrainian power facilities with BlackEnergy 3 and KillDisk.
deterring'. This has, in more recent years been accompanied by ‘dissuasion by denial’, which posits deterring an action by having the adversary see a credible capability to prevent him from achieving potential gains adequate to motivate the action. China, Russia and the United States are still largely short of the pre-conditions for achieving these in cyberspace, in large part due to their lack of basic cyber hygiene that would otherwise dissuade or even deny access. Of the two, dissuasion may offer the most promise in slowing, discouraging, and, in the event of failure, detecting activities. In the interim, however, deterrence in cyberspace seems to be occurring largely in the form of what some Chinese analysts call ‘deterrence by punishment’. This is akin to the U.S. Department of Defense definition of ‘deterrence by cost imposition’ and manifests itself in the three following ways in the context of China, Russia, and the United States:

1. For the United States, ‘deterrence by punishment’ is conducted through sanctions. Examples include the U.S. imposition of sanctions against five members of China’s People’s Liberation Army (PLA) for their alleged industrial cyber espionage leveraged against U.S. companies in 2015 and against the Russian government for alleged targeting of the U.S. election in 2016. While reliant on detection, this form of deterrence is more focused on the back end of the equation, namely retaliation for engaging in hacking activities. As punishment, political and economic costs to one’s adversary are meant to deter such activities from occurring in the future.

2. For China, ‘deterrence by punishment’ is conducted through exfiltration. Examples include the alleged actions of Chinese entities in accessing SF-86 clearance forms stored by the U.S. Office of Personnel Management (OPM), revealing personal information on 25 million U.S. federal employees in 2015. During this incident, China’s domestic hackers surpassed U.S. estimates. The punishment in this scenario derives from the fact that the data on employment history, financial


---


19 Forensic reports on a range of similar cyber intrusions and attacks within the information and kinetic spheres indicate that most facilities commit the same errors in terms of basic hygiene. While it may be challenging to thwart highly tailored and expensive campaigns as with the use of Stuxnet against centrifuges in the Iranian Natanz nuclear facility, alleged employment of a worm to disrupt India’s INSAT-4B satellite and the Korea Hydro and Nuclear Power facilities, as well as the growing appearance of a new strain of wiper called Hidden Cobra to target financial, media, and aerospace critical infrastructure suggest that both the basics of cyber security and resiliency are still lagging behind. Until realized, at the strategic level, it is difficult to argue for effective “deterrence by denial” to counter cyber intrusion and attack. At the tactical level, the list of basic hygiene practices that could be applied is lengthy, but often lacking at the facilities that have been compromised. It includes such foundations as 1) improved mapping and monitoring of logs and baseline activities, 2) restriction of remote data storage and access, 3) vetting and accountability for contractors and vendors, 4) disabling of U.S.B ports in the industrial environment and enabling of analogue back-up systems, 5) monitoring and controls for jump boxes between corporate and industrial systems, 6) encryption of data at rest and in transit, 7) expanded training and pen-testing of end-users to mitigate the impact of social engineering, 8) greater segmentation and limitation of privileged access to limit damage when particular end users are compromised, 9) restrictions on BYOD within the industrial and corporate environment, 10) updated plans for containing and recovering from incidents, and perhaps most importantly 11) whitelisting could be applied more widely at facilities that have relatively few operations to perform.

background, regional contacts, as well as family and friends could be used to deter one’s adversary from political or other courses of action via the coercion or blackmail.

(3) For Russia, ‘deterrence by punishment’ is conducted through interference. Examples include alleged Russian cyber tampering in the U.S. elections during 2016 that has laid bare and exacerbated fissures in democratic institutions and social cohesion within the United States. As in the case of China, Russian influence again transcended U.S. expectations. Only, in this case, the spectrum was much broader than simply federal employees. This bears similarities to Russian accusations against Washington for its alleged interference in Ukraine’s political system. The punishment in this scenario is tied to the impacted state deadlocking itself from within, making effective and coherent retaliation difficult.

These three frames suggest that Chinese, Russian, and U.S. deterrence operations are primarily operating in the information security sphere. Still, there are also examples of kinetic damage or the threat of such destruction wrought through cyberspace. For the United States, its alleged targeting of Iran’s Natanz nuclear facilities caused physical damage and disruption to the operation of its centrifuges and nuclear program. For China, its alleged targeting of Lockheed Martin and Boeing data is widely thought to have enhanced its fighter jets and other weapon systems used in its own military hardware and in sales to conflict-prone regions. For Russia, its alleged targeting of Ukraine’s energy facilities resulted in a wiping of critical operational data and damage to the functionality of the nation’s power grid.

While these cases have had an indirect impact on the relations among the three countries, apart from the Chinese example of industrial espionage allegedly leveraged against U.S. military contractors, they are not necessarily directly countering one another. Moreover, they do not directly impact one another’s nuclear capabilities. Nonetheless, espionage in the nuclear sphere to locate weaknesses and areas of exploit are widely thought to be ongoing. The open source information on such activities is scant, but reports and workshops held jointly by such groups as Chatham House and Stanley Foundation indicate the scope of concern and potential vulnerabilities.

This is even more so the case as remote data storage, inspection devices, monitoring systems, and other equipment utilized in nuclear facilities are updated and converted into a digital format. Recognizing the enhanced reliance of nuclear facilities on digitization and remote data storage, including for delivery and guidance systems, Chinese, Russian, and U.S. sources are understandably focused on a similar set of capabilities in cyberspace. This confluence suggests that ‘deterrence by punishment’ will increasingly transition from information to kinetic cases.

As just one example, Chinese analyses of how to deter in cyberspace have already begun to cross the bounds of defensive into offensive operations, including: (1) strengthening encryption of sensitive data in transit, particularly through quantum communications, (2) implementation of more red team military exercises, (3) reduced reliance on external software and hardware supply chains, (4) expansion of the number of smart weapon platforms, (5) implementation of electromagnetic capabilities and systems, (6) strengthening of joint operations and command and control in the face of cyber-attack, (7) enhancement of information management accuracy, and (8) restricting, weakening, severing, destroy, and inflicting chaos on an opponents’ systems.
Such priorities can also be found in Russia and the United States.

Considering these trends, asymmetry among these countries in cyberspace is diminishing. Their ability to conduct defensive and offensive cyber operations are converging, as are the threats that they face. There is no question that the role of individuals and groups that are often labelled as patriotic hackers may disrupt these state-to-state relations through their own activities. However, the impact of these cases may not be as lasting as in the nuclear realm. One example comes from the U.S. targeting of five PLA members with sanctions and the political disruption following the cyber intrusion and mass data exfiltration from OPM. Unlike the 1998 release of the Cox report following the alleged Chinese theft of U.S. nuclear warhead designs, these incidents in cyberspace did not permanently derail talks between China and the United States.

On the contrary, these cyber incidents could be said to have provided greater impetus for China-U.S. dialogue at an even higher level. In fact, their relations in cyberspace have proven to be more resilient than those of Russia and the United States. This was reflected in the U.S. response to the OPM hack that only condemned individual hackers within China, contrasted with U.S. official reaction to alleged election tampering that sanctioned the Russian government. While faring better than Russia, China’s takeaway from these incidents is that a country must first possess such capabilities for the United States to acknowledge its position and status. Mounting a sufficient threat towards Washington is what gamers respect, bringing it to the table. As in the case mentioned above on North Korea, this contradicts long-held beliefs that cyberspace is entirely opaque or lacks attribution. To realize deterrence in cyberspace, a country must be able to demonstrate its ability to carry out an attack or retaliation. And it requires a degree of transparency to do so.

Beyond often-overlooked transparency in cyberspace, another set of trends compelling China, Russia, and the United States to engage on cyberspace challenges stems from the fact that the capabilities that they pursue and the threats that they face are increasingly similar. The cases discussed above show that each party has served as both an attacker and victim in cyberspace, thereby diminishing the Chinese argument that any one country can maintain cyber superiority above all others. If anything, the more dependent upon cyberspace that these countries become, the more that they are opening themselves up to disruption and attack. While seemingly destabilizing, this mutual vulnerability also opens channels for discussing strategic stability.

**Strategic Stability and Mutual Vulnerability**

As we shift towards confronting more kinetic cyber operations, deterrence frameworks remain largely rooted in the information domain. This transition provides an opportunity to revisit strategic stability in cyberspace. Unlike the nuclear sphere, where it remains a debated precept, mutual vulnerability in cyberspace is self-evident. While there remains no open source information that the three countries have actively used cyber means to target one another’s nuclear arsenal, this form of reconnaissance is more than likely. As such, it is incumbent upon those researching this field not to narrow their definitions of what constitutes a nuclear weapons system, since there are many digital information and operation platforms that support nuclear deployment and are vulnerable to cyber intrusion and attack.

Efforts have begun, particularly in the United States, to explore these trends. Yet, within China, analysts within the cyberspace and nuclear research fields remain largely isolated
from one another. While each community is researching strategic stability, Chinese cyber experts and nuclear experts have embarked upon these studies separately, with a limited grasp of each other’s challenges and findings.\(^{21}\) Russian analysts also note that domestic military doctrine and debate largely excludes discussion of cyber deterrence or cyber weapons as part of its conventional arsenal.\(^{22}\) Thus, while a great deal of time and energy is devoted in both China and Russia to researching and potentially imitating the U.S. ‘third offset strategy’ (第三次抵消战略) and ‘cross-domain synergy’ (跨领域集成), stove-piping is occurring not only among these countries, but also within them.\(^{23}\)

Overall, these trends act as an impediment to enhancing our understanding of how information deterrence and cyber deterrence are defined and operate. China, Russia, and the United States are understandably cautious about drawing road maps to their cyber vulnerabilities, particularly within their nuclear arsenals and relevant platforms. Yet there remains room for greater research into how expanded transparency and diminished asymmetry are shaping mutual vulnerability and strategic stability in cyberspace. To better understand these trends, areas of further research include the following:

(1) **Terminology:** Chinese writings on cyberspace indicate that deterrence (威慑), containment (遏制), and coercion (威逼) are often used interchangeably. As in the nuclear realm, these terms merit greater analysis for the contexts in which they are applied. On Russia and the United States, while efforts have been made to create bilateral cyber glossaries, their differences in both terminology and operations contribute to misunderstandings and escalation. Thus, in addition to a multilateral glossary that incorporates the varied definitions of the various countries engaged in cyber operations, the field would benefit from an anonymized and generic review of cyber incidents that have already occurred. This would offer an analytical foundation with greater granularity than in the Tallinn Manual and with greater inclusivity than found among North Atlantic Treaty Organization countries.

(2) **Technology:** Reviews of forensic reports indicate how there is still a wide gap in how each country’s technical community measures the sophistication of tactics and nature of a cyber intrusion versus an attack. While even state-initiated cyber-attacks may utilize lower grade tools, such as commonly available Poison Ivy malware, there are other methods and signatures that merit a more streamlined technical analysis. This was evident in the U.S. national intelligence assessment of 2016 election-related cyber incidents that jumbled the names of hacking groups.
malware, and signatures. Yet, it also appears across any number of forensic reports that research the methodology behind cyber intrusions and attacks, using different metrics and labels in doing so. Just as multiple independently targetable vehicles, hypersonic glide, enhanced range, cruise missile, and other capabilities provide measure of a country’s advances in the nuclear sphere, the complexity of and overlap among cyber-attacks and actors could be better synthesized by providing analysis that synthesizes this scattered technological discussion.

(3) **Targeting:** Enhanced understanding of how targets are evaluated in cyberspace is also crucial. As opposed to nuclear deterrence in which counter-force and counter-value targets are used to differentiate how a country engages in nuclear first-strike or retaliation, in cyberspace the distinction between civilian and military targets, as well as regular facilities and critical infrastructure remains murky. While it may be premature to anticipate a concrete delineation of how these different realms are targeted, at a basic level, determining how each of these countries delineate critical infrastructure in cyberspace is crucial for understanding how to define deterrence in cyberspace. Focusing on the target provides a better sense of the aims, intent, and even the source of a cyber-intrusion or cyber-attack.

In sum, while incidents occurring in the nuclear domain indicate the inherent difficulty of China, Russia, and the United States engaging in meaningful official exchange on mutual vulnerability and strategic stability, cyberspace offers underappreciated levels of transparency and symmetry. As a result, many of the rigidities that have hindered nuclear exchange among these three countries may be less of a long-term constraint in cyberspace. Thus, while strategic stability may look different in the cyber domain, its unique composition could offer a more solid foundation for future exchanges. Setting up the basic groundwork of Chinese, Russian, and U.S. terminology, technology, and targeting represents an essential first step for better understanding how cyber deterrence may operate in the future.

Dr. Lora Saalman is Director of and a Senior Researcher in the China and Global Security Programme at the Stockholm International Peace Research Institute (SIPRI).