Divergent U.S. and Chinese Views of Information, Deterrence, and Future Warfare

By Dean Cheng

When it comes to activities in the information domain, much of the public's attention has been focused on its information extraction activities. Hacking of U.S. government databases, such as the Office of Personnel Management (OPM) as well as various corporations have tended to dominate the American public's discourse on information activities by the People's Republic of China (PRC). But understanding the reasons and strategy underlying China's actions is essential, for this context shapes the Chinese approach to information and information technologies, which includes artificial intelligence, quantum computing, and space operations.

How China Sees Information and Future Power

From the perspective of the leadership of the Chinese Communist Party (CCP), information and the associated technologies, have become a foremost part of a nation's power. Information and communications technology (ICT) have permeated all aspects of society, and become an integral part of a nation's infrastructure.[1] The elevation of information and associated technologies is termed "informationization (*xinxihua*; 信息化)."

Consequently, for the CCP, information is now seen as ***inextricably linked to both the broader national interest, as well as to regime (or at least CCP) survival***. It is important to note here that this is *not* simply about the role of information in wartime. The Chinese leadership is not solely focused how information might be applied in a military conflict; rather, they see it as being a determinative factor in the ongoing competition among states writ large.

This, as Chinese writings emphasize, is because of the ascendant role of information in the 21st Century's economic and political realities. In their view, we are living in the Information Age, and the ability to gather accurate information in a timely manner, transmit and analyze it, and then rapidly exploit it, is the key to success. These abilities are the centerpiece of any effort to achieve "information dominance"—the ability to gather, transmit, analyze, and exploit information more rapidly and accurately in support of one's own ends, while denying an adversary the ability to do the same.

As economies and societies have informationized, Chinese analysts have concluded that threats to national interests and security have also become informationized. Countries not only have unprecedented access to each others' economies, but also can seek to influence the broader population and top decision-makers. Indeed, information itself can constitute a

[1] Tan Wenfang, "The Impact of Information Technology on Modern Psychological Warfare," *National Defense Science and Technology*, No. 5 (2009), p. 72.

threat, whether by eroding the morale of key decision-makers, or being altered (such as by viruses) to devastate key networks and infrastructure.

These threats extend beyond information networks (e.g., vulnerability to denial-of-service attacks) and component computers (e.g., computer viruses, malware). Instead, the very information itself can constitute a threat, if, for example, its content erodes the morale of key decision-makers, popular support for a conflict, or the will of the military to fight. Consequently, China's interpretation of its national interests has expanded, in step with the expanding impact of information writ large on China.

At the same time, however, the free flow of information constitutes a dire potential threat to CCP rule. While the Chinese Communist Party may no longer emphasize ideological arguments of "from each according to their ability, to each according to their needs," it remains firmly committed to its role as the "vanguard party," and therefore, the sole legitimate political authority in the PRC. It also likely sees the collapse of the Soviet Union as a consequence of the failure to retain the "vanguard party" role, and as important, the liberalization of informational controls. The policies of *glasnost* and *perestroika*, of opening and reform, led to the downfall of the other major Communist Party. Just as information is the currency of economic and military power, it is also the basis for political power.

This *maodun* (矛盾), or conundrum, sets the stage for the second key assumption. As an authoritarian party, and with the fate of the Communist Party of the Soviet Union as an object lesson, the CCP cannot afford to allow the free flow of information. This would allow too many challenges to its rule. ***The Chinese leadership therefore will seek to control the flow of information***.

To some extent, efforts at exerting this control are merely sustaining longstanding policies. The CCP has long demonstrated a willingness to employ extravagant lengths, such as the massive organizational infrastructure to support censorship, to limit that flow. However, because of the nature of the Information Age, including extensive interconnections and linkages across various information networks, the CCP cannot only control the flow of information ***within*** China. Instead, it must also control the flow of information ***to*** China.

This effort to control the external flow of information constitutes a fundamental, qualitative change in how nations approach information as a resource. Of course, states have long sought to shape and influence how they are portrayed. Nor is limiting access to outside information a new phenomenon. However, the Chinese efforts, in light of their views of the qualitative changes wrought by the rise of the Information Age, are different in scale and scope. Controlling information now means limiting not just newspapers and television programs, but the functioning of the Internet, on a global scale.

Some of this may be achieved through technical means. The "Great Firewall of China," for example, is a major undertaking to examine, in detail, the data streams that are trying to enter the PRC. Chinese state-run telecoms reportedly hijack and redirect portions of the Internet that are not normally intended for Chinese destinations.

But China's efforts are not limited to the technical side. The effort to influence, if not control, the functioning of the Internet extends to how the PRC looks upon the international system, including the governance of the international common spaces. ***If the Chinese are***

going to control and influence information flow to China, then it will have to shape and mold the international structures which manage that information flow. This is not to suggest that China is about to overthrow the current system. Chinese writings regularly note that the PRC is still in the period of "strategic opportunity," which China needs to exploit, if it is to improve itself, and elevate itself to the ranks of middle-developed powers.[2] Thus, China must continue to pursue policies of peaceful development and interaction.

As China has grown steadily more powerful, though, it has increasingly questioned the underlying international structures that more and more often constrain its behavior. These structures, as Chinese writings note, were often formulated without input from the PRC. A reviving China, as well as a CCP intent on staying in power, increasingly chafes at these externally imposed limitations.

Nonetheless, challenging the current structure assumes greater urgency as ***the PRC, and especially the CCP, also sees itself as increasingly in competition with the other major powers, especially the United States***. It is the United States that champions Internet freedom and, more broadly, the free flow of information. Moreover, as many Chinese officials have argued, it is American policies that encourage China's neighbors to challenge Chinese hegemony over its littoral waters, or help sustain the Dalai Lama and other sources of internal instability.

This does not mean that the PRC believes that war or armed conflict is inevitable. Indeed, there is no reason to think that, in the short-term (the next decade or so), that the PRC would actively engage in an armed attack on its neighbors. Unlike the Cold War, there is no "Fulda Gap" scenario to concentrate upon.

At the same time, the Chinese leadership is well aware of the utility of pursuing its ends through a variety of means, including "hybrid warfare." China has demonstrated an ability to employ fishing boats and civilian law enforcement vessels to pursue its territorial agenda. If Chinese warships are not shooting at foreign craft, Chinese fishing boats have had fewer compunctions about physically interfering with foreign vessels' operations. The world's information networks, where attributing actions are much harder, would seem to be the ideal environment for waging the kind of gray conflict typical of hybrid warfare.

Therefore, at the strategic level, the PRC will be constantly striving to shape both domestic and foreign views of itself through the information that it transmits and projects. Meanwhile, it will be trying to determine and dictate how others view China, as well as identifying their strengths and weaknesses. These efforts are no different than how every state behaves, in terms of collecting intelligence about potential allies and adversaries.

Where the PRC has diverged from other states' practices, however, is their growing focus on dominating the information-space in both peacetime and wartime. In particular, Chinese efforts to establish information dominance, while somewhat constrained in peacetime by the

[2] See Yuan Peng, "China's Strategic Opportunity Period Has Not Ended," *People's Daily Online,* July 31, 2012, available at http://en.people.cn/90883/7893886.html; and, Xu Jian, "New Changes in the Next Decade of China's Period of Strategic Opportunity," *Guangming Ribao,* October 30, 2013, available at http://cpc.people.com.cn/n/2013/1030/c83083-23372744.html; and, Zhang Yunling, "Deeply Considering the International Environment Confronting Our Nation's Period of Strategic Opportunity," *Seeking Truth,* December 18, 2015, available at http://theory.people.com.cn/n1/2015/1218/c83846-27946374.html.

international system, are likely to be more comprehensive as well as much more pronounced in event of war.

This is reflected in Chinese military developments of the past several years, which are themselves ***the culmination of nearly a quarter century of thought regarding the shape and requirements of future warfare***. The Chinese concept of "informationized local wars" reflects this ongoing evolution, with its focus on the role of information in all aspects of future warfare. This concept grows out of the lessons initially derived from observing the allied coalition in the first Gulf War of 1990-1991, leavened with observations from the Balkan wars of the 1990s and the American invasions of Afghanistan and Iraq. Thus, the PLA initially conceived of future wars as "local wars under modern, high-technology conditions," but then concluded that not all high-technology was equally important.

With the conclusion that information technology is the foremost element of high technology, reflecting the larger strategic shift from the Industrial Age to the Information Age, the PLA has subsequently developed new doctrine, to link its concept of future wars to the kinds of forces it will field and the kinds of operations they will conduct.

From the Marxist perspective of the CCP, the growing importance of information technology in economics and society inevitably influences the nature of warfare. Informationized societies and economies lead to informationized wars, which in turn require informationized militaries to fight them successfully. In informationized warfare, information serves as both a force multiplier for people, materiel, and capability, as well as a form of combat power itself. Older weapons that are modernized with modern sensors and communications equipment (e.g., the B-52 and the A-10, or adding laser guidance modules to "dumb bombs") can retain or even enhance their effectiveness. Improved command and control systems can better coordinate various forces. Better information can allow more effective allocation of limited resources, allowing one's own forces to be more flexible and agile. Information weapons, such as computer viruses, in turn, can paralyze an opponent's system-of-systems, causing them to disintegrate and decohere.

CCP lessons derived from observing other peoples' wars, especially those of the United States but also Russia, has led the CCP and PLA to further refine its views on future warfare. From an initial focus on network warfare, electronic warfare, and psychological warfare, it is now apparently emphasizing command and control warfare, and intelligence warfare. The implication would seem to be that not all networks, electronic systems, or leaders are equally important; instead, those in key decision-making roles, and the people and systems that inform their decisions, should be higher priority targets. It is important to note here that this does not mean that the PLA will neglect other networks, systems, or personnel (e.g., logistics, combat units) in its pursuit of winning future informationized wars. Rather, it reflects priorities for allocating resources and developing capabilities.

This may be seen in the efforts of the last several years in fielding various types of new equipment and improved joint training. Alongside new fighters, warships, and self-propelled artillery are an array of new unmanned aerial vehicles, electronic warfare platforms, and sensors. The massive reorganization of late 2015 and early 2016 marks a major waypoint in this steady effort to prepare the PLA "to fight and win future local wars under informationized conditions," and what the PLA subsequently revised to "informationized local wars."[3]

Especially important is outer space. One of the key domains of Hu Jintao's "New Historic Missions" for the PLA (alongside the maritime and electromagnetic domains), the PLA clearly views the ability to establish "space dominance (*zhitian quan*; 制天权)" as a key element of future "informationized local wars."[4] But space is important not as a place or domain, but because of its role in gathering, transmitting, and allowing the exploitation of information. Consequently, efforts to establish space dominance are not necessarily focused on anti-satellite missiles or co-orbital satellite killers. A special operations force that can destroy a mission control facility, or an insider threat that can insert malware into a space tracking system, are as much means of achieving space dominance.

Deterrence Behaviors

For both the United States and the People's Republic of China (PRC), this increasingly tense security situation places a growing emphasis on deterrence. Unfortunately, the two states define "deterrence" differently, and have very different approaches which entail very different risk calculus.

As the primary guarantor of the international order, the United States has global responsibilities and commitments. It is therefore in the American interest to forestall, or deter, threats to that international order. In order to realize this deterrence in defense of the global order, the United States maintains a global military presence, which is in turn supported by a network of space and information systems that allow the United States to conduct expeditionary operations far from its shores. At the same time, a key element of American security thinking is preserving the American homeland from nuclear attack, a task which requires maintaining global surveillance through space-based sensors linked through information systems.

The PRC has long primarily focused on defense of the homeland, including deterrence of nuclear and conventional attack. As its economy has grown, however, to the current point where it is the second largest economy, it has developed an expanding array of global economic interests. While the People's Liberation Army (PLA) remains primarily a regional military, it has been charged with "new historic missions" which include deterring threats against these expanding economic interests.[5] To this end, the PLA has been improving its capabilities which, coupled with its revamped organization, suggest a growing global presence as well.

[3] David Finkelstein, "China's National Military Strategy: An Overview of the 'Military Strategic Guidelines,'" in Roy Kamphausen and Andrew Scobell, eds., *Right-Sizing the People's Liberation Army: Exploring the Contours of China's Military* (Carlisle, PA: Strategic Studies Institute, 2007), p. 96.

[4] Academy of Military Science Military Strategy Research Office, The Science of Military Strategy (Beijing, PRC: Military Science Publishing House, 2013), pp. 146–147.

[5] Daniel M. Hartnett, "The 'New Historic Missions': Reflections on Hu Jintao's Military Legacy," in Roy Kamphausen, David Lai, and Travis Tanner, eds., *Assessing the People's Liberation Army in the Hu Jintao Era* (Carlisle, PA: U.S. Army War College Press, 2014), pp. 33-34.

This situation suggests that the United States and the PRC are likely to encounter each other more and more, raising the prospect for increased friction. At the same time, both sides have an interest in deterring conflict, especially with each other but with other states as well. These deterrence activities will involve not only the traditional nuclear realm, but increasingly the outer space and information/cyber domains. Unfortunately, the two states also have fundamentally divergent views of deterrence itself. This converging interest yet divergent understandings has distinct implications for regional and global stability.

Diverging Concepts of Deterrence

Part of the problem confronting the two states rests in their very different conceptions of deterrence. Western analysts have tended to link deterrence with dissuasion. Thomas Schelling, for example, in his 1966 book *Arms and Influence*, specifically defines deterrence as "the threat intended to keep an adversary from doing something," and distinguishes it from compellence, which is defined as 'the threat intended to make an adversary do something." [6] The two, for Schelling, are distinctly different.

Glenn Snyder makes the same point by noting that deterrence "is the power to *dissuade* as opposed to the power to coerce or compel."[7] Thus, Western analyses of deterrence implicitly (and even explicitly) associate deterrence with dissuasion, *and disassociate it from compellence or coercion*.

By contrast, the Chinese term *weishe*, while translated as "deterrence," embodies both the concepts of *dissuasion* and *compellence*. As one Chinese volume notes, the concept of *weishe* is associated with the idea of bending the adversary to one's own will, both in terms of dissuading them from doing what they would like to do (deterrence) ***and*** making them do what they do not wish to do (compellence).[8] The 2011 PLA volume on military terminology describes the deterrent strategy as "a military strategy of displaying or threatening the use of armed power, in order to compel an opponent to submit."[9] It is similarly agnostic on whether the submission is in terms of dissuading or coercing.

Another key difference between Western and Chinese views of deterrence rests on whether it is seen as a goal or a means. For many American analysts and strategists, deterrence is often seen as a goal, especially in terms of deterring an adversary from acting in a given domain (e.g., cyberspace), or with particular weapons (e.g., nuclear deterrence).

By contrast, Chinese analysts are focused more on the political situation, with deterrence in any domain or with any weapon system seen as a *means* to achieving political ends, rather than as a *goal*, in and of itself. Success in deterring or dissuading an adversary from acting in space or cyberspace, is secondary to success in obtaining the previously established political

[6] Ibid., p. 69.

[7] Glenn Snyder, "Deterrence and Defense," in Robert J. Art and Kenneth N. Waltz, eds., *The Use of Force* (New York: University Press of America, 1988), p. 31. Emphasis added.

[8] National Defence University Science Research Department, *New Perspectives on Military Transformation: Explaining 200 New Military Concepts* (Beijing, PRC: PLA Press, 2004).

[9]All Army Military Terminology Management Committee, Academy of Military Sciences, *Chinese People's Liberation Army Terminology* (Unabridged Volume) (Beijing, PRC: Military Science Publishing House, 2011), p. 51.

goal. If, for example, Beijing could affect reunification with Taiwan by acting in space, that would be successful deterrence (or coercion). But if Beijing could affect reunification without acting in space, that would ***also*** be acceptable. The goal is reunification, not acting (or not acting) in a given domain.

These differences in thinking about deterrence are further compounded by what would appear to be a very different threat and risk calculus in Beijing from those of the United States and Soviet Union. The United States and the Soviet Union and their respective alliances generally avoided direct confrontations between their armed forces. As important, there were few territorial issues that entailed the two sides' forces threatening conflict. (The status of Berlin in the early Cold War era period arguably comes closest.)

China's ongoing standoff with India suggests a very different approach towards interactions with other nuclear-armed powers. Chinese forces have crossed the Line of Actual Control (LoAC) between China and India several times since 2013. While there has been no violence, the military forces of both the PRC and India have been involved in the various confrontations in the area of Arunachal Pradesh and more recently the Doklam Plateau and near Dok-la. The very idea of dispatching military forces across a demarcation line separating two nuclear-armed powers suggests that there are very different dynamics and considerations at work in Beijing than has historically been the case in Washington or Moscow.

Chinese Conceptions of Nuclear, Information, and Space Deterrence

For the PRC, its history and resources have led to diverging views of deterrence. These different views, as well as the very different information environment of the 21st century, pose major challenges for the U.S.-PRC relationship that overlap the nuclear, space, and cyber realms. Given the different Chinese view of both deterrence and nuclear risk management, it is important to consider how the PRC thinks about not only the three realms, but the interplay among them.

Nuclear Deterrence (he weishe; 核威慑)

Chinese writings on nuclear deterrence suggest that Beijing's views in this vital arena also differ significantly from those of the West.

In one respect, the Chinese view is reassuring. For several decades, China's views seem to be consistent with a nation that is fielding a minimal or limited nuclear deterrent. There is no publicly available evidence that Chinese analysts are interested in nuclear counterforce targeting. As important, China's force structure, even with its ongoing modernization program, does not suggest development of such a capability. The United States (and Russia) therefore do not necessarily have to worry about a Chinese effort to destroy their nuclear forces in their silos and on their bases. This may be changing, as the PRC has built hundreds of silos in its western desert, and appears intent on fielding a much more substantial nuclear force.

As important, Chinese writings on nuclear deterrence have consistently called for the ability to wage "real war (*shi zhan*; 实战)" with nuclear weapons, in addition to implementing deterrence. "Deterrence capability is based on the ability to wage real war, and the structure of deterrent strength is indistinguishable from combat strength. Deterrent strength is embedded in real combat capability."[10] In other contexts, such as space and cyber operations, "real war" means the ability to conduct actual military operations, as opposed to demonstrations or signaling, so this suggests that there is at least some PLA interest in the implementation of nuclear operations and strikes.

The interplay of "real war" and deterrence are intertwined in what appears to be a concept of an escalation ladder as part of Chinese deterrent activities. In the PLA volume *Science of Second Artillery Campaigns*, the authors suggest that the Second Artillery (and presumably the PLA Rocket Forces) has adopted an array of actions, in escalating order, to frame their deterrence activities.[11] The rungs comprise:

- *Public opinion pressure*. This is the public display of Chinese nuclear missiles and other capabilities to the media, to underscore to foreign audiences China's nuclear deterrent capability.
- *Elevating weapons readiness*. Because Chinese nuclear warheads appear to be stored at centralized facilities, and are not necessarily regularly installed atop missiles, this rung incorporates increasing readiness of both warheads and launchers. Thus, demonstrating launch preparations is one element, but also deploying warheads to missile units might be a Chinese move as well.
- *Displays of actual capability*. This goes beyond public displays before the media, to include invitations to foreign attaches to inspect Chinese forces, coverage of high-level visits to forces in the field, especially during exercises, and military reviews and parades. It might also include deliberate deployment of mobile systems out of garrison while adversary surveillance systems are known to be watching. It might also include launch exercises, on their own or incorporated into broader exercises.
- *Manipulating tensions and creating impressions and misimpressions*. By deploying forces, emitting various signals and signatures, simulating launches, and/or raising readiness (in a demonstrable fashion), the PLA would seek to influence an adversary's calculus of the likelihood and destructiveness of a conflict.
- *Demonstration launches*. A higher rung on the Chinese deterrence ladder is to conduct actual missile launches at designated land or sea areas (not directly against an adversary). Such launches might involve a variety of systems (e.g., ballistic and cruise

[10] Academy of Military Science Military Strategy Research Office (PRC), *The Science of Military Strategy* (Beijing, PRC: Military Science Publishing House, 2013), p. 147.

[11] This section is drawn from Chinese People's Liberation Army Second Artillery, *The Science of Second Artillery Campaigns* (Beijing, PRC: PLA Publishing House, 2003), pp. 281-296.

missiles, or different types of MRBMs), to underscore the varied nature of Chinese capabilities, and the comprehensive readiness of Chinese missile forces.

- *Demonstration launches near an adversary's forces or territory*. By engaging in test firings near an adversary's naval forces, homeland, or seized territories, the PLA would be trying to coerce an adversary into abandoning their ongoing activities. It is a form of indirect attack that seeks to deter or coerce.
- *Announcing the lowering of the nuclear threshold*. The PLA specifically associates this move with countering an adversary that has substantial nuclear capabilities, but also an advantage in high-technology conventional weapons. In order to counter the latter element, the Chinese leadership might announce a lowering of the nuclear threshold, e.g., entertaining a nuclear response to conventional attacks against vital strategic targets in the PRC. These include nuclear facilities (including nuclear power stations); targets that could cause great loss of life such as hydroelectric facilities (presumably such as the Three Gorges Dam); the nation's capital or other major urban or economic centers. Such an adjustment might also occur if the PRC found itself in a situation where it was losing a conventional war and was faced with a challenge to its national survival.

This "escalation ladder" or "deterrence ladder" underscores the Chinese belief that successful deterrence requires the PLA to be able to signal resolve. Similarly, it also reflects the Chinese focus on affecting an adversary's assessments and psychology, as much or more than the fielding of specific capabilities.

Information Deterrence (xinxi weishe; 信息威慑)

This approach suggests that China will integrate elements of "information deterrence (*xinxi weishe*; 信息威慑)" into their approach towards nuclear deterrence, and vice versa. Information deterrence is defined as a type of "information operation activity (*xinxi zuozhan xingdong*; 信息作战行动)" that can either display one's information advantage or announce deterring information to compel an adversary to abandon their willingness to resist, or to reduce the strength of their resistance.[12] It involves, at some level, threats against enemy information systems, such as to paralyze or disrupt them, to constrain enemy actions and thereby help achieve one's political goals.

Consistent with the Chinese view, noted earlier, that deterrence is not about dissuading activities in one or another domain or involving a particular class of weapons (nuclear, information), but in order to achieve a previously determined set of political goals, Chinese writings on both information deterrence and deterrence writ large do not emphasize deterring activities ***in*** information space. Rather, Chinese writings on information

[12] All Army Military Terminology Management Commission, *Chinese People's Liberation Army Terminology*, op. cit., p. 262.

deterrence discuss the use of information operations to ***effect*** deterrence. Information deterrence is about achieving deterrent goals *through* information operations.

Information deterrence, like nuclear deterrence and the broader concept of *weishe*, incorporates both dissuasion as well as coercion. Consequently, Chinese information deterrent actions are aimed at achieving a particular political goal by undermining the adversary's will, rather than preventing an attack on Chinese information systems. The Chinese goal is to influence an adversary's cost-benefit calculations, making them question whether their preferred course of action is worth likely damage incurred from attacks on their information networks and systems. Ideally, Chinese deterrent actions would persuade the target that the cost of non-compliance is too high, and it would be easier to accede to China's preferred course of action. Essentially, the Chinese concept of information deterrence is the use of informational means, whether attacks on information systems and networks or certain types of information itself, to erode the adversary's willingness to resist.[13]

From the Chinese perspective, information's growing role in warfare means that threatening access to information can deter and coerce an informationally comparable adversary. The degree of Internet penetration in military, political, and economic affairs allows unprecedented access to foreign infrastructure. The potential ability to massively disrupt an adversary's entire society creates deterrence opportunities. Indeed, on a day-to-day basis, states already engage in information deterrence, precisely because the scale of disruption that would otherwise erupt would be enormous. Few states are confident that their defenses could prevent such disruptions.[14]

Chinese writings note that cyber strength is not necessarily correlated with conventional capabilities. That is, a state might have relatively weaker conventional capabilities yet have strong network warfare capabilities that could nonetheless disrupt or even paralyze their conventionally stronger adversary. On the other hand, a side with weak set of information capabilities may be less able to effect information deterrence, even if they have relatively stronger conventional forces.[15]

If this is applied to the nuclear realm, then this suggests that the Chinese have a very different concept of nuclear crisis management. Where the U.S. and Soviet Union saw transparency as providing certain stabilizing effects in the nuclear context, the Chinese would seem to view uncertainty and ambiguity as preferable. Indeed, it may be that the Chinese would see the denial of information, whether collection or transmission, as strengthening deterrent effects. An adversary who is uncertain of China's capabilities is more likely to be deterred. Similarly, an adversary who is uncertain of whether it can exercise command and control of its nuclear weapons is also likely to be deterred—or coerced.

[13] Chinese Military Encyclopedia 2nd Edition Editorial Committee, *PLA Encyclopedia, 2nd Edition, Military Strategy* (Beijing, PRC: China Encyclopedia Publishing 2007), p. 283.

[14] Academy of Military Science Military Strategy Research Office, *The Science of Military Strategy,* op. cit., p. 196.

[15] Academy of Military Science Operations Theory and Regulations Research Department and Informationized Operations Theory Research Office, *Informationized Operations Theory Study Guide* (Beijing, PRC: Military Science Publishing House, November 2005), pp. 15-16.

This set of views, in turn, affects both computer network exploitation (CNE), as well as computer network attack (CNA) and defense (CND), as applied against NC3. Because information and associated networks are so important in the event of conflict, mapping these networks and otherwise understanding a potential adversary's information systems requires extensive computer network reconnaissance, which in turn must happen in advance. According to Chinese analyses, this means that there will necessarily be significant CNE in peacetime. As important, by penetrating an adversary's networks, and letting them know that one has done so, one can potentially not only dissuade but even coerce them. Indeed, evidence of successful penetration can be an important element of *weishe*, since an adversary cannot be certain of the extent of said penetration, or whether Trojan horses or other malware might have been left behind.

In the Chinese view, CNE therefore complements a demonstrated CNA capability. The ability to enter an adversary's networks is necessary, in order to engage in any kind of computer network attack. At the same time, a demonstrated capability of undertaking CNA, even if not employed in a given crisis, will nonetheless make the adversary wary.

In the Chinese view, network offensive operations (which include but are not limited to CNA) are the foundation of information deterrence.[16] They can be used to attack a variety of targets, threatening much of an adversary's society, economy, and military. Such operations are hard to defend against, in some ways harder than conventional, nuclear, or space attacks. In the event of a crisis, threats of information attacks (e.g., computer viruses) will affect an adversary's will, and may persuade them to cease resistance.

The lack of experience with large-scale network offensive operations also enhances deterrence. In the Chinese view, the uncertainty about the ultimate effects of network attacks is a factor forestalling large-scale network conflict.[17]

At the same time, Chinese analysts believe the ability to successfully defend and safeguard one's information resources and systems can also deter an adversary, by limiting their ability to establish information dominance. Without information dominance, the enemy cannot easily establish dominance over other domains (e.g., air, space, maritime), raising the costs to achieve their broader strategic objectives. They are therefore likely to be deterred from initiating aggression or may be coerced into submitting.

All of this suggests that the Chinese may try to apply CNE, CNA, and CND capabilities against an adversary's NC3 systems, as a complement to nuclear deterrence missions. Reconnaissance of those systems demonstrates an ability, and interest, in penetrating those networks, which raises questions about their reliability. This affects the ability to detect attacks, exercise command and control of forces, and assess damage.

Even if China does not actually damage any such systems in peacetime, the possibility that NC3 networks may harbor malware is likely to influence crisis and wartime decision-making. This possibility is made more real if there is a demonstrated ability to engage in damaging network attacks in other environments (or against other states). The resulting

[16] Ibid., p. 15.

[17] Academy of Military Science Military Strategy Research Office, *The Science of Military Strategy,* op. cit., p. 190.

reduction in stability in turn may also deter or coerce an adversary, by making them question how far they are willing to risk further deterioration.

A particular point of vulnerability is an adversary's space systems. A vital part of information deterrence, especially in the nuclear context, is the space element.

Space Deterrence (kongjian weishe; 空间威慑)

In the Chinese view, space deterrence is the use of space forces and capabilities to deter or coerce an opponent, preventing the outbreak of conflict, or limiting its extent should conflict occur. Space deterrence is possible because of the growing importance of space-derived information in not only military but economic and social realms. By displaying one's own space capabilities and demonstrating determination and will, the PLA would hope to induce doubt and fear in an opponent over the prospect of loss of access to information gained from and through space, and the resulting repercussions. This, in turn, would lead the adversary to either abandon their goals, or else limit the scale, intensity, and types of operations.[18]

It is important to note here that the Chinese concept of space deterrence is not focused on deterring an adversary from conducting attacks against China's space infrastructure, per se. Instead, it is focused on employing space systems as a means of influencing the adversary's overall perceptions, in order to dissuade or compel them into acceding to Chinese goals. Thus, it is not so much deterrence ***in*** space, as deterrence ***through space means***.

Space capabilities are seen as contributing to overall deterrent effects in a number of ways. One is by enhancing other forces' capabilities. Thus, conventional and nuclear forces are more effective when they are supported by information from space-based platforms, such as navigational, reconnaissance, and communications information. This makes nuclear and conventional deterrence more effective, and therefore more credible.

In addition, though, space systems may coerce or dissuade an opponent on their own. Space systems are very expensive and hard to replace. By holding an opponent's space systems at risk, one essentially compels them to undergo a cost benefit analysis. Is the focus of Chinese deterrence or coercive efforts worth the likely cost to an adversary of repairing or replacing a badly damaged or even destroyed space infrastructure? Moreover, because space systems affect not only military but economic, political, and diplomatic spheres, damage to space systems will have wide-ranging repercussions.[19] Is the target of Chinese deterrent or coercive actions worth the impact of the loss of information from space-based systems on other military operations, or on financial and other activities? The Chinese clearly hope that the adversary's calculations would conclude that it was better not to challenge Chinese aims. Even the threat of interference, and disruption of space systems "will impose

[18] Zhou Peng and Wen Enbing, "Developing the Theory of Strategic Deterrence with Chinese Characteristics," *China Military Science*, Vol. 3, No. 20 (2004), p. 20; and, Academy of Military Science Military Strategy Research Office, *The Science of Military Strategy*, op. cit., p. 181.

[19] Li Jingjun and Dan Yuquan, "The Strategy of Space Deterrence," *China Military Science*, No. 1 (2002).

a certain level of psychological terror, and will generate an impact upon a nation's policy-makers and associated strategic decision-making."[20]

This conception of space deterrence operations has clear implications for the nuclear realm. The ability to damage the space portion of an adversary's NC3 networks (including communications and reconnaissance) will affect not only their ability to counter China, but other states as well. Thus, in the case of the United States, it would affect the American ability to deter Russia and North Korea. Interestingly, China's lack of a space-based missile early warning network would suggest that this is an asymmetric vulnerability, where China is less liable than either the United States or Russia.

PLA teaching materials suggest that there is a perceived hierarchy of space deterrence actions, akin to the nuclear "escalation ladder," involving displays of space forces and weapons; military space exercises; deployment or augmentation of space forces; and employment of space weapons.

- *Displays of space forces and weapons* (*kongjian liliang xianshi*; 空间力量显示) occur in peacetime, or at the onset of a crisis. By demonstrating space capabilities, an adversary is ideally dissuaded from escalating a crisis or pursuing certain courses of action, because their space capabilities will be potentially put at risk. The demonstrations should be accompanied by political and diplomatic gestures as well. The goal, notably, is not to prevent an adversary from acting *in space*, but from acting *at all*.
- *Military space exercises* (*kongjian junshi yanxi*; 空间军事演习) are undertaken as a crisis escalates, if displays of space forces and weapons fail to compel an adversary to change their behavior. Both physical and tabletop/computerized exercises can be part of this rung, so long as they demonstrate capabilities and signal readiness. Examples include ballistic missile defense tests, anti-satellite unit tests, exercises demonstrating "space strike" (*kongjian tuji*; 空间突击) capabilities, and displays of real-time and near-real-time information support from space systems.
- *Space force deployments* (*kongjian liliang bushu*; 空间力量部署) reflect a major escalation of space deterrent efforts. This rung involves deploying additional forces, and adjusting the location of already deployed forces. For satellites, any repositioning is a major activity, because it consumes fuel necessary to maintain operational positioning and therefore affects mission assurance. This rung can also involve the recall of certain space assets, such as space planes and space shuttles, both to secure them from possible attack and to prepare them for new taskings. This rung occurs if an adversary is believed to be preparing for war, and reflects one's own preparation for combat
- The final rung in Chinese writings on space deterrence is "*space shock and awe strikes"* (*kongjian zhenshe daji*; 空间震慑打击). If the three previous, non-violent deterrent

[20] Academy of Military Science Military Strategy Research Office, *The Science of Military Strategy,* op. cit., p. 181.

> measures are insufficient, then the PLA suggests engaging in punitive strikes involving aerospace forces. These are intended to warn an adversary that failure to back down will lead to full-blown conflict—not just in space but terrestrially as well. Such strikes are described as "the highest, and final technique" (*zuigao xingshi he zui hou shouduan*; 最高形式和最后手段) in deterring and dissuading an opponent. Employing hard-kill methods, soft-kill methods, or a combination, one would attack an opponent's physical space infrastructure or data links, respectively. The goal is to induce psychological shock in opposing decision-makers, leading them to cease their activities. If it fails, an opponent's forces will nonetheless have suffered some damage and losses, and be weakened relative to one's own forces.

These Chinese writings on space deterrence clearly suggest that there may be a willingness to consider operations against an adversary's space-based information and surveillance networks, employing both hard-kill (e.g., kinetic anti-satellite systems) and soft-kill (e.g., cyber) methods. Such moves might be withheld until the highest stage of a crisis, but the interest in "space shock and awe strikes" suggests a search for the most psychologically damaging space targets. The space component of the NC3 infrastructure may be a logical target for such strikes.

How Chinese Conclusions Will Shape Chinese Actions

Given these Chinese perspectives and conclusions, there are certain implications that arise, which are reflected in Chinese behavior.

Chinese actions must be holistic and will be comprehensive. The PRC still sees itself as a developing country. Despite being the second-largest GDP in the world, this must be spread over a population of 1.3 billion. As important, China is not necessarily wealthy; while it has enormous untapped human and physical potential, until that is converted into actual capacity and capability, much of China will remain poor. In this light, the Chinese are likely to pursue more of a whole-of-government approach, if only to leverage its available resources. Thus, whereas the United States has both a military and a civilian space program (the latter divided into three substantial segments), China is unlikely to pursue such a strategy that demands extensive redundancy and overlap.

This will likely be reinforced by the high priority accorded informationization in general. While various senior level efforts have been halting at times, Xi Jinping has clearly made informationizing China a major policy focus. Insofar as the Chinese see their future inextricably embedded in the Information Age, these efforts will enjoy highest level support, with efforts to reduce stove-piping and enhance cross-bureaucracy cooperation. This, in turn, will mean not only greater cooperation within the military, but also between the military and the other national security bureaucracies, as well as with the larger range of Chinese ministries, and both public and private enterprises.

Chinese actions are determined by Chinese priorities and are unlikely to be heavily influenced by external pressure or blandishments. If the Chinese leadership sees information as integral to national survival, and views economic espionage as part of the process of obtaining necessary information, then it will not be easily dissuaded. Similarly, insofar as the Chinese leadership links information flow with regime survival, Beijing will also restrict and channel information flow in ways that meet internal security requirements. To this end, the targets of Chinese actions will have to impose very high costs on Beijing, so that the gains are not worthwhile to the PRC, if they seek to alter the Chinese approach.

The difficulty of influencing Beijing is exacerbated by the Chinese leadership's sense that it is already in a strategic competition with various other states. The CCP perceives challenges to its security stemming not only from the United States, but also from Russia, India, and Japan, as well as certain non-state actors such as Uighur and Tibetan separatists. Indeed, it is essential to recognize that the Chinese leadership sees itself as already engaging in multilateral deterrence—a position it has adopted since at least the 1960s, when it believed it was facing threats from both the Soviet Union and the United States.

Chinese views about the extent of threats are further reinforced by the reality that the information space is both virtual and global; it is therefore not currently restricted by any national borders. For the Chinese leadership, controlling information flow and content therefore entails operating not just within the Chinese portion of information space, but globally. It requires accessing foreign information sources and influencing foreign decision-makers, while preventing outside powers from being able to do the same in China.

As a result, ***the PRC is undertaking an increasing array of actions beyond its own borders, striving to dominate what had previously been part of shared spaces***. This applies not only to information space, such as the Internet, but also physical domains such as the seas and outer space. Indeed, one can see parallels among Chinese efforts to dominate the South China Sea, its growing array of counter-space capabilities, and its efforts to control and dominate information space. In each case, the PRC is intent upon extending Chinese sovereignty, including its rules and its administrative prerogatives, over what had previously been open domains.

In this regard, Chinese actions are justified by a very different perspective on the functioning of national and international law. Indeed, Chinese views of legal warfare occur in the context of a historical and cultural view of the role of law that is very different from that in the West. At base, the Chinese subscribe to the concept of rule ***by*** law, rather than the rule ***of*** law. That is, the law serves as an instrument by which authority is exercised but does not constrain the exercise of authority.

In the broadest sense, pre-1911 Chinese society saw the law from an instrumental perspective, i.e., a means by which authority could control the population, but not a control extended over authority. Laws were secondary to the network of obligations enunciated under the Confucian ethic. The Legalist "school" of ancient China placed more emphasis on the creation of legal codes (versus the ethical codes preferred by the Confucians), but ultimately also saw the law as a means of enforcing societal and state control of the population. No strong tradition ever developed in China that saw the law as applying to the ruler as much as to the ruled.

During the early years of the PRC, Chinese legal development was influenced by the Marxist perspective that the "law should serve as an ideological instrument of politics."[21] Consequently, the CCP during the formative years of the PRC saw the law in the same terms as imperial China. The law served as essentially an instrument of governance but not a constraint upon the Party, much less the Great Helmsman, Mao Zedong. In any case, the Party exercised rule by decree, rather than through the provision of legal mechanisms. Mao himself, during the Cultural Revolution, effectively abolished both the judiciary and the legal structure.[22] Since Mao's passing, while there have been efforts at developing a body of laws, most have been in the area of commercial and contract law. Moreover, the law remains an instrument that applies primarily to the masses as opposed to the Party, i.e., the law exists to serve authority, not to constrain it.

This has meant that the Chinese government employ laws, treaties, and other legal instruments to achieve their ends, even when they fly in the face of traditional legal understanding or original intentions. Thus, the Chinese do not see their efforts to extend Chinese authority over shared spaces as inconsistent with international law, but as part of political warfare; opposition to their efforts is similarly seen as an effort to contain China and to threaten CCP rule.

Consequently, Chinese efforts to dominate information space strive not only to control the flow of information, but to delegitimize the idea of the information realm as a shared space, accessible to a variety of groups. Chinese authorities have striven to limit the role of non-state players in setting the rules for the Internet. At the same time, it has also sought to limit the access of dissidents, Taiwan political authorities, Tibetan activists, and others who have tried to oppose China's position to not only Chinese audiences, but global ones. Given the Chinese leadership's view of the existential threat posed by information (whether inside or outside China), such efforts are perceived as defensive efforts aimed at preserving the regime.

China is likely to pursue a form of informational isolationism. The Chinese solution to the challenge of information vulnerability is to restrict the flow of information. This is not intended to replicate the extreme North Korean form of isolation, but to align information flows ideally "with Chinese characteristics." Indeed, Beijing strives to make itself informationally autarkic, wholly self-dependent in terms of information access, information generation, and information transmission. Thus, the PRC has created Chinese versions of information companies, is pursuing a homegrown semiconductor industry to substitute for imported computer components, and otherwise tries to limit informational access to and from China.

This is an ironic rejection of the very macroeconomic policies of the past four decades that have allowed China to succeed and advance. But, just as the CCP accepts performance costs in the speed of the Chinese Internet (imposed by the nature of the Great Firewall of

[21] Eric W. Orts, "The Rule of Law in China," *Vanderbilt Journal of Transnational Law*, Vol. 34, No. 1 (November 2001), p. 57.

[22] Murray Scot Tanner, *The Politics of Lawmaking in China* (Oxford, UK: Clarendon Press, 1999), p. 43; and Dwight Perkins, "Law, Family Ties, and the East Asian Way of Business," chapter in Lawrence E. Harrison and Samuel P. Huntington, eds., *Culture Matters* (NY: Basic Books, 2000), p. 235.

China), they accept the economic and innovative opportunity costs that are imposed by the broader restrictions imposed on information flow. This is a dangerous bargain, however, as CCP leaders appear to be trading longer term economic growth for short-term stability and curbing immediate challenges to their authority. If the Chinese leaders are correct that future development of "comprehensive national power (CNP)" is directly tied to the ability to exploit information, then their actions are likely, in the long run, to actually limit future CNP growth.

It is important to note, however, that this isolationism does not mean closing China off from the rest of the world's information. Reports that China actively redirects and hijacks entire segments of the Internet to Chinese servers (presumably for later examination and analysis) highlight that Chinese leaders want to control what comes into China, not simply exclude it.[23] As important, they are willing to undertake actions that affect, and could alienate, many other states and actors in pursuit of this end.

Conclusion

In the wake of the Russian invasion of Ukraine, it is clear that the concept of deterrence needs to be thoroughly reexamined. Biden administration comments that American threats of sanctions were intended to deter, even while also acknowledging that they probably would not, highlights the difficulties of effecting deterrence against a determined adversary, even when the states arrayed against it outmatch it economically and militarily.

Deterring the PRC (specifically the CCP) will be even more difficult. While the United States and the West developed some common terms of reference and shared concepts with the Soviet Union over the four decades of the Cold War, the same cannot be said of the PRC. China's strategic context and history in Asia are totally different from the shared Western experience across the East-West divide. The PRC also has substantially more financial resources than the Soviets, and is more enmeshed in Western economies.

Most notably, however, the PRC has been devising a systematic approach towards the role and application of information, in the form of "informationized" development and informationized warfare. Coupled with Chinese thinking about political warfare (which is the application of information at the strategic level), this makes the CCP a very different, and far more formidable, adversary.

Deterring the PRC will require employing a similarly comprehensive array of techniques and means. It will require that we better understand both the vulnerabilities and strengths of their approach to information, and the same in our own societies.

Mr. Dean Cheng is a Senior Research Fellow, Chinese Political and Security Affairs at the Heritage Foundation.

[23] Chris Demchak, Yuval Shavitt, "China's Maxim – Leave No Access Point Unexploited: The Hidden Story of ChinaTelecom's BGP Hijacking," *Military Cyber Affairs*, Vol. 3, No. 1 (2018).