Intersect, Vol 14, No 1 (2020)

The Cyber-Nuclear Nexus in East Asia: Cyberwarfare's Escalatory Potential in the US-China Relationship

Will Matheson
Harvard College

Warfare in the digital age poses distinct challenges to the lessons of the 20th century. From outer space to cyberspace, the domains in which conflict now spills and the tools with which conflict will occur have evolved, carrying implications for national security strategy. The vast majority of cyber operations pertain to issues of cyber espionage, especially of an economic nature, and thus hold little significance for grand military strategy. However, evolution in cyberspace has created concerning implications for how militaries think about strategy and great power competition. Most critically, cyber operations may now influence both technical capacities and decision-making in the nuclear domain. As a result, this emerging cyber-nuclear nexus must be better understood by civilian and military leaders alike.

With changing geopolitics, scholars are increasingly interested in understanding the possibility for conventional conflict between the US and China the ability for such a conflict to "go nuclear." Growing perceptions of an emerging "new Cold War" between the two nations hold a key implication for nuclear stability – just as the Cold War with the Soviet Union saw a series of nuclear crises (for example, Suez 1956, Berlin 1961, Cuba 1962, the Sino-Soviet Border Crisis of 1969, and the Able Archer crisis of 1983-4), the emergence of true great power competition will likely bring conflicts over hotspots such as Taiwan or the East and South China seas. However, the bodies of scholarship investigating the risks of Sino-American conflict have thus far insufficiently considered concepts of the cyber-nuclear nexus. This paper seeks to remedy this gap by understanding how aspects of China's cyber warfighting doctrine and the technical capacities of cyber warfare shape US-China escalation scenarios. It finds that, though substantial ambiguity remains around cyber warfighting capabilities and doctrines, potential cyber attacks on nuclear command, control, and communications (NC3) could generate both substantial fog of war effects and create secret advantages for the cyber attacker that could embolden dangerous risk taking during a brinksmanship crisis between the US and PRC. In particular, China's cyberwar doctrine may introduce serious instability to future crises.

This essay proceeds in four parts. First, it provides technical clarification on the nature of cyber weaponry. Second, it explains the theories supporting the cyber nuclear nexus. Third, it explains both America's and China's cyber warfighting doctrines. Fourth, it unites these sections in explaining how the technical nature of cyber weapons, the general theory of the cyber-nuclear nexus, and an understanding of specific cyber warfighting doctrines together influence escalation scenarios between the US and China.

Understanding the Nature of Cyber Weaponry

One of the main areas of consensus among cyber warfighters is that the technical nature of the tools in this domain favor offensive action. As a result, just as countries favor development of nuclear weapons and delivery systems over defensive tools like ballistic missile defense, so too do they favor offensive cyber operations (OCOs) over attempts to defend against cyber-attacks. The cyber domain by nature favors the attacker, who can scour any technology platform for backdoors; only once such backdoors are found can they be patched or otherwise mitigated, meaning defenders are always playing catch-up. The sheer cost of defense compared to the relative inexpensiveness of offense, as well as the proliferation of attack surfaces with technological development, thus drive offensive dominance in the cyber realm (Mussington, n.d.). As a result, almost all countries adopt pre-emptive cyber strategies that rely on offensively minded doctrines.[1]

Casual understandings of cyber operations often glean this point about offensive dominance yet fail to understand the nature of cyber weaponry. Just as sea or air are domains in which militaries deploy many different weapons with different strengths and purposes, so too is the cyber domain. Given the recency of the rise of cyberwarfare, the accelerating pace of capabilities growth in this domain, and the secrecy around it, academic research will struggle to fully encapsulate the expanding scope of this realm and the true variety of weapons within it. However, Smeets proposes a useful framework for delineating between types of OCOs. First, he explains that OCOs serve one of two types of strategic value: either support for national security strategy, or ability to produce specific outcomes in specific conflicts or instances of state competition. When casual observers think of OCOs, they commonly think about them in the context of the former value set. However, the bulk of OCOs are far better understood in the latter set: they will not provide a form of "final arbitration" in geopolitical conflict, but rather have operational utility below that threshold just as navies, air forces, and armies likely would not have an independent decisive effect on a conflict (Smeets, 2018).

Additionally, to borrow terms from the literature pertaining to nuclear weapons, OCOs can have either counter force, or counter value,

[1] For example, see (Grigsby, 2017; Herpig, 2018)

use. Examples of counter force cyber capabilities (CFCCs) include Russia's disabling of Georgian forces in its 2008 invasion and Operation Orchard, Israel's use of the Suter program to disable Syrian air defenses when it bombed the Al-Kibar nuclear reactor in 2007. Examples of counter value cyber capabilities (CVCCs) include the Stuxnet virus used to undermine Iran's nuclear program and Russia's shutting down of the Ukrainian energy grid in 2014. Generally, CVCCs have standalone value. For example, Stuxnet offered an alternative between doing nothing toward Iran's nuclear program and launching a bombing campaign, because it was calibrated and used separately from any other action such that it would not provoke a kinetic escalatory response (Smeets, 2018).

In contrast, CFCCs most often operate as force multipliers, integrated into broader, often kinetic operations. Given their asymmetric nature, they integrate particularly well with other military tools as they can equalize or significantly disrupt conventional power imbalances. CFCCs can be used as force multipliers in two ways. "Pooled interdependence" refers to their use separately from conventional forces such that different operations cumulatively overwhelm the enemy; Russia's deployment of cyber weapons in Georgia and Ukraine particularly embodies this approach. Alternatively, CFCCs may be integrated into a "sequential interdependence" approach where conventional and cyber operations directly rely on one another to succeed, making the approach more prone to operational failure but also augmenting the level of force multiplication. Israel's Operation Orchard embodies this strategy, as the bombing of the Al-Kibar reactor by Israeli planes directly relied on the successful disabling of Syria's air defenses. Notably, the CVCC examples still play a quasi-military role, showing how the distinction between CFCCs and CVCCs is not absolute (Smeets, 2018).

Finally, by nature, cyber weapons must be secret until their use. Should an attacker have hacked into an enemy network, thereby granting them the ability to execute an OCO, they cannot broadcast their possession of this OCO to the enemy, who would quickly patch the vulnerability once becoming aware of it. Deterrence requires credible threats, often borne out of transparency, yet cyber weapons by nature cannot meet such a threshold. This trend is called the cyber commitment problem – a would-be attacker cannot disclose the possession of a cyber weapon for the purpose of deterrence or coercion without sacrificing such a weapon (Gartzke & Lindsay, 2017). OCOs are thus tools for winning conflict, not deterring it – their inherent nature is asymmetric and unknown until their use.

To summarize, then, cyber weapons by nature favor offensive action rather than defense against cyber weapons and only work as long as their existence is concealed from the target. They are poor tools for final arbitration of a conflict, but they can be effective as strategic tools to achieve specific outcomes. Cyber weapons can also be separated into CFCCs, which serve strategic value in military operations as force multipliers, an CVCCs, which often are used independently and operate at a level of conflict perceived as below the threshold of military action.

The Logic of the Cyber-Nuclear Nexus

This background information on the nature of OCOs will help illuminate the deficiencies in the literature explaining cyberwarfare's effects on conflicts and will help specify how cyber can influence nuclear escalation scenarios. A common argument made about OCOs is that their escalatory potential is overblown. Much of the literature either unfairly puts the burden of strategic decisiveness on cyber weapons as if they were analogous to nuclear weapons, or assumes that because previous cyber operations have failed to kill people, they are not sufficiently dangerous. While many of these accounts are fairly weak, Bordhard and Lonergan provide one of the most compelling arguments for this perspective. They argue that the difficulty of having OCOs prepared to strike specific targets at a moment's notice, the limited and uncertain effects they have, the opportunity cost of using backdoors in the future instead, the monetary cost of developing OCOs, and the limited ability for OCOs to cause lethal damage together limit their escalatory potential (Borghard & Lonergan, 2019). Their argument makes a lot of sense, given a scenario in which a bolt-of-blue, standalone OCO were launched. However, their analysis fails to speak to the use of CFCCs as force multipliers - they assume no interdependence between all of the other tools the military holds at its disposal. Assuming states view cyber as a battlefield domain in a vacuum separate from other domains ignores both the technical capacity for integration and the empirical record. Especially in crisis situations, the integration of conventional, nuclear, and cyber domains will add greater interactivity and minimize cost considerations. Additionally, Bordhard and Lonergan's argument implies less escalatory potential for poorer states and non-state actors: if costs are prohibitive to wielding a sufficiently deep and sophisticated arsenal of OCOs, resource-rich states like the US, China, and Russia will dictate the future of OCO integration into military strategy. To their credit, Bordhard and Lonergan do concede toward the end of their article that cyber's escalatory potential is greatest where stakes are high and at least one state involved in a conflict believes it needs to escalate (Borghard & Lonergan, 2019). However, the impulse to disregard this scenario ignores the most dangerous aspect of future cyber operations, as they could significantly complicate hotspot escalation and brinksmanship crises.

Fortunately, academics have begun to devote more attention to the logic of a cyber-nuclear nexus. The most common explanation for cyber warfare's influence on nuclear behavior suggests that integrated CFCCs may impede the use of critical networks and their nodes during the onset of a crisis, fostering a fog of war – i.e., impaired situational awareness during a military operation as information becomes unclear or distorted. In particular, there are four ways OCOs could create this problem: by disrupting communications, such that the two sides do not interpret signals the same way; by creating use-em-or-lose-em mentalities among forces with predelegated launch authority should NC3 be disrupted; by triggering an irrational or otherwise poor response by key leaders as severed NC3 creates a specter of complete military defeat, fostering panic; and by creating an impression that the timeframe of the crisis has been compressed, pressuring leaders to act immediately. In each of these scenarios – which would likely occur simultaneously – the use of cyber pre-emption during the initial stages of a conflict might exacerbate its escalatory potential in subsequent stages. These scenarios for fog of war pose a distinct threat to crisis stability, given the crucial importance of clear thinking and accurate assessment during a nuclear crisis (S. J. Cimbala, 2016).

Additionally, concurrent developments may augment cyber warfare's influence on the logic of nuclear deterrence. Improvements in ballistic missile defense and anti-air defense, as well as better kinetic capabilities like Precision Global Strike to eliminate weapons delivery systems, exacerbate cyber's threat to a secure second strike (S. J. Cimbala, 2017). Recent work questioning force survivability during the Cold War and into the present further add credibility to the disarming potential of a coordinated military operation employing a robust mix of tools, including OCOs (Long & Green, 2015). While the efficacy of some of these technologies remains questionable, the broader trend implies innovation in non-cyber warfare realms has interactive effects with the cyber-nuclear nexus. As a result, these integrated actions could exacerbate the panic that leaders would experience as a result of the fog of war.

Admittedly, the fog of war scenario relies on an assumption of some irrationality. Fog of war scenarios suggest compromised NC3 will cause irrational escalation, but leaders, if rational, will realize they have misread the strategic balance of power during a nuclear crisis such that they miscalculated their position of weakness, leading them to de-escalate (Gartzke & Lindsay, 2017). However, assumptions of rationality are dangerous, particularly given the acute stress under which those in the nuclear chain of command operate (Dougherty, 1987). A reasonable takeaway might be that context and leadership matter in nuclear crises, but that at a baseline, the fog of war effects of cyberwarfare pose a risk of escalation that warrants attention. Note that future discussion of "balance of power" in this paper refers to strategic, i.e. nuclear balance of power as a term of art used to understand brinksmanship crises.

Beyond the fog of war scenario, a second cyber-nuclear escalation risk exists: Gartzke and Lindsay propose a theory for escalation based on how the inherent nature of cyber weapons undermines successful brinksmanship during nuclear crises. The idea of assured retaliation dominates discourse on nuclear strategy – with it, a nation can credibly pose the threat of mutually assured destruction to other nuclear-armed states. In theory, because of assured retaliation, countries can engage in brinksmanship crises, so long as transparency ensures each side knows how far it can "push" the other. However, as the previous section explained, cyber weapons must be kept secret until their use – they are tools for winning, rather than warning. At the cyber-nuclear nexus, then, these weapons merge realms of great instability (cyber) and stability (nuclear), creating ambiguity with interactive effects for both realms. With regard to the cyber realm, the stability-inducing role of nuclear weapons should, in theory, generate a stability-instability paradox that creates an upper bound on cyber provocations. As a result, the influence of nuclear weapons theoretically enables a greater scope of cyber aggression at lower levels of conflict intensity. Conversely, in the nuclear realm, cyber warfare potentially undermines nuclear stability precisely because of its secrecy. Cyber weapons as unknown tools of winning can substantially alter the nuclear balance of power, but do so as long as only the possessor of the cyber weapons knows of their existence. As a result, because the target of the OCO has no knowledge of it – and, by extension, the altered balance of power – the risk of deterrence failure in a brinksmanship crisis substantially increases. Cyber operations present the opportunity to prevent an enemy from detecting an attack until it is too late, as well as prevent the enemy's ability to retaliate. That substantial power means the would-be cyber attacker has an advantage that allows it to never have to back down, while the other side responds to risk taking by its adversary in kind, under the incorrect assumption that an equal balance of power still exists. However, as risk escalates, both sides will be increasingly likely to view the situation through the lens of deterrence failure, which could trigger catastrophic results (Gartzke & Lindsay, 2017).

To add to the destabilizing effects, a possessor of a cyber weapon may have doubts about its ability to fully incapacitate an adversary's nuclear or conventional capabilities. At a high level of uncertainty, this may stabilize the cyber-nuclear nexus as the possessor would reject the cyber tool outright. However, with only a moderate degree of uncertainty, the possessor would face incentives to launch a kinetic, preemptive strike in conjunction with the cyber operation in order to ensure its efficacy – a move that would exacerbate instability. Additionally, should the target of an OCO detect the compromise of its systems but fail to have an ability to mitigate or neutralize its effects, it will face extreme "use-em-or-lose-em" pressures. Should the defender detect and mitigate the attack, it still may be destabilizing, as the defender would then read its adversary's intentions as far more hostile, which could cause a spiral of increasingly aggressive behavior in a crisis as each side reacts in-kind to the initial display of preemptive aggression. This effect can even happen without the attacker actually attempting a compromise, should the defender detect and mitigate a false positive compromise (Gartzke & Lindsay, 2017).

To summarize, cyber warfare can disrupt nuclear-induced stability in two ways. First, the "fog of war" theory explains how the various uses of OCOs against critical systems can generate destabilizing psychological effects, leading to irrational escalation. The effects can thus push a middling crisis into a brinksmanship crisis, or can destabilize an existing brinksmanship crisis itself. Second, the "balance of power" theory suggests that while cyber is traditionally bounded by the stabilizing influences of nuclear weapons, at the onset of brinksmanship crises the influence of the cyber realm instead introduces a serious destabilizing factor to conflict resolution as each side engages in risk taking based on different assumptions of the balance of power between the two states. In this scenario, the brinksmanship crisis must already be occurring, given that it is premised on the alteration of perceived strategic balance of power in such a crisis.

Both of these escalation scenarios employ the logic of CFCCs as preemptive, disarming tools focused on NC3. However, the logic of destabilization behind both arguments similarly applies to targets beyond NC3. These OCOs may target battle management, command, control and communications (BMC3) networks as well. In such cases, the attacker would likely use the OCOs as a prelude to, or directly integrated with, a campaign aimed at suppressing missile defenses (S. J. Cimbala, 2017). The effects of these attacks would likely create psychological conditions similar to those created by attacks on NC3 systems.

Additionally, OCOs could be used as disabling preemptive measures in a "left of launch" operation. In either nuclear or conventional contexts, OCOs need not only target NC3/BMC3 – they may also target the delivery systems themselves. Delivery systems are easier (and therefore more reliable) to target with OCOs, for four reasons. First, these systems are a far greater attack surface than NC3, ranging across both delivery systems types and the range of activities accessing these systems from initial design to ongoing maintenance. Second, air gapping is far less common on delivery systems than on warheads themselves. Third, vast modernization efforts that many powers are currently undertaking are leading to greater digitization of these forces, making them easier to penetrate. Finally, statements by the DOD itself have expressed concern over the risk of OCOs in left of launch operations (Wasson & Bluesteen, 2018). When considering the cyber-nuclear nexus, these attacks complement attacks on NC3/BMC3, pooling effects to potentially create destabilizing scenarios. Together, cyber threats to NC3 and BMC3 and left of launch cyber operations demonstrate how a wide range of cyber weapons can be used to paralyze an enemy in ways that generate significant fog of war/fears over a counterforce strike and/or alter the balance of power without the enemy knowing of such an alteration.

Assessing the Technical Validity of these Theories

The logic of the cyber-nuclear nexus rests on a key assumption regarding the technical capacity for cyberweapons to access such critical targets, which many may initially dismiss as unrealistic. If the evolution of cyber truly poses a threat to their nuclear networks, practitioners know better than to broadcast such a fact, complicating a fair assessment of the true threat cyber warfare poses. Nevertheless, a careful assessment of their signals lends credibility to the logic of a cyber-nuclear nexus. As early as the 1980s, the Joint Chiefs of Staff identified serious weaknesses in the US NC3 system that could have been exploited in ways that would have denied critical information to strategic command (*A Historical Study of Strategic Connectivity, 1950-1981*, 1982). In addition, the US invested heavily in counterforce capabilities and planning during the Cold War. Operation Canopy Wing explicitly sought to compromise the NC3 system of the Warsaw Pact should a crisis situation demand it. Those in the Warsaw Pact viewed this program as American willingness to launch a disabling first strike, and reacted by developing the Perimeter program that automated a retaliatory nuclear launch, regardless of the status of Soviet NC3. These programs illustrate how seriously nuclear powers sought advantages relating to NC3 systems, and suggest that governments are willing to aggressively invest in such programs (Gartzke & Lindsay, 2017).

More recently, in 2013, then-Commander of the United States Strategic Command Robert Kehler testified before Congress on the status of the NC3 system, claiming, “we are very concerned with the potential of a cyber-related attack on our nuclear command and control and on the weapons systems themselves" (Kehler, 2013. 10). Additionally, a 2015 GAO study reported on the existence of known capability gaps in the US’s NC3 system, which implies unknown capability gaps as well (US Government Accountability Office, 2015). Beyond direct statements by the government, a RAND study produced to advise the US Army Cyber Command on how to better integrate CCFCs advocates for the targeting of command and control systems with OCOs to support kinetic aspects of an operation (Porche III et al., 2017. 69). Together, this evidence illustrates both the strong empirical record of states’ emphasis on counterforce capabilities and the weaknesses permeating even the most secure NC3 structures.

Realistically, the discussion of the cyber-nuclear nexus likely consists of two extremes – those who claim cyber is hyped and poses no real threat, and those who see cyber as the master key that will lead to a total collapse of nuclear systems. The truth likely exists somewhere in between. Given the rapid evolution of cyber capabilities, grey zones in cyber space, poorly understood interactivity, and the secrecy surrounding the cyber domain, ambiguity dominates much of this conversation; as such, academics would do well to not overestimate too greatly toward one extreme or the other, recognizing that cyber operations certainly pose a real danger without allowing for alarmist fantasies to capture the imagination.

Before concluding this section, two important notes. First, the key distinction drawn in the preceding pages between CFCCs and CVCCs demonstrates how a sizable chunk of the literature dismissing the destabilizing threat posed by OCOs is misplaced by only considering CVCCs. As explained in this section, CFCCs, integrated into military operations as force multipliers, should be investigated when understanding how cyber warfare alters nuclear balances. However, CVCCs may in the future become truly destabilizing. Future development of Big Data and its AI outputs may make them so fundamental to the functioning of society that independent cyber threats may generate coercive or deterrent effects, wielding strategic value analogous to nuclear weapons (Stephan, 2020). Indeed, nations like China, India, and Russia have recognized the tremendous potential in AI and have developed serious national strategies to capture its advantages (Horowitz et al., 2018). Such considerations thus may influence great power competition in the future.

Second, one weakness of this body of literature as a whole is that it remains bounded to the realms of technological capability and the general logic of nuclear crises – it has thus far insufficiently questioned how these dilemmas may manifest in relationships between specific nuclear powers. This omission is understandable, given the limited information on both the technological and doctrinal sides of this question and the nascence of this body of literature. However, given the indications from practitioners in the field that the cyber-nuclear nexus merits legitimate concern, scholars should recognize the need for understanding how the evolution of cyber warfare capabilities and doctrines will influence specific nuclear dyads. As such, this paper will now investigate how such developments alter the Sino-American relationship, by explaining China's cyber warfare doctrine and then applying it to these theories of the cyber-nuclear nexus.

Cyber Warfare Doctrines in China and the United States

Given the importance of secrecy in cyber warfare capabilities, it is unsurprising that states do not disclose much information relating to their cyber warfare strategies. Generally, the US is seen as the most transparent, including congressional testimony by key members of the military, US STRATCOM publications, and the DOD's release of a cyber strategy every few years. Given the US's first-movers advantage in this space and the greater availability of information, its cyberwarfare doctrine is associated with what "conventional" thinking on cyberwarfare strategy should be.

The 2018 DOD Cyber Strategy is the most recent government articulation of the US's cyber warfighting doctrine, and illustrates a pivot toward more aggression in cyberspace. At its outset, it embraces cyber as necessary for winning great power competition with Russia and China, echoing the strategic pivot outlined in the 2017 National Security Strategy. The document makes explicit that OCOs will be integrated into other theaters during wartime or conflict, reflecting the logic of CFCCs. Additionally, it argues that adversaries the US will face will also rely on CFCCs, meaning a key priority for cyber warfighting is to exploit other nation's warfighting reliance on the cyber realm. For both of these needs, the US is accelerating its development of OCOs, and embraces a posture of "defending forward" in which these offensive operations are necessary to the maintenance of stability in key hotspots and crises (Department of Defense, 2018). Similarly, the Trump administration's National Cyber Strategy underscores a need to bolster US capabilities and impose greater consequences in cyberspace (White House*, 2018)*.

Recent evidence confirms this slight shift in US cyber doctrine toward a more aggressive posture. Based on comments from then-National Security Advisor John Bolton, in 2018 the classified National Security Presidential Memorandum 13 (NSPM 13) delegated the ability to conduct OCOs further down the military chain of command as part of an effort to preempt threats by adopting a more aggressive posture at lower levels of conflict. This posture also encourages faster reactions to provocations in cyber space (Nakashima, 2018; Rudesill, 2018).

In contrast to the US, the CCP/PLA provides almost no information regarding its cyberwarfare doctrine. Beyond general needs for secrecy, historically China may not have even had a coherent cyber warfare doctrine: complicated, overlapping apparatuses between CCP leadership, the PLA, and the PRC, and regulation of cyber-related technology by six different agencies all fostered a lack of communication and centralized decision-making. Moreover, the nature of general PLA bureaucratic politics suggests its many secretive cyber agencies likely did not communicate with one another and instead engaged in turf wars (Lindsay, n.d.). However, the 2015 creation of the Strategic Support force as a branch of the PLA to harmonize all cyber warfare efforts may have remedied this problem and helped generate a more coherent doctrine (Defense Intelligence Agency, 2019). Given the dilemma with limited information on China's cyber doctrine, the proceeding paragraphs will use the very limited available sources in order to sketch as accurate an approximation as possible.

China's cyber doctrine has evolved over the previous three decades, gradually becoming more refined as its cyber warfighting capabilities improved. According to Jiang Tianjiao, a Chinese academic at Shanghai International Studies University, China has undergone three distinct phases of doctrinal evolution. Based on an analysis of both military and non-military sources (particularly those close to the CCP's Leading Small Group (LSG) for Cybersecurity and Informatization, the key body in China coordinating cybersecurity policy), Jiang believes China embraced a concept of offensive dominance and always striking first from the 1990s up until 2008. At that point, as scholars began to pay attention to cyber warfare and China's capabilities developed, a debate ensued between the offensive dominance theorists and those embracing cyber deterrence, with the latter camp ushering in the current phase of China's doctrine around 2015 that formalizes the pivot to deterrence and defense. This shift reflected a gradual understanding of how CFCCs integrate into kinetic operations, recognizing that while OCOs present great asymmetric power, an offensive doctrine still would guarantee some form of retaliation. In other words, Chinese analysts recognized cyber warfare is not a panacea for military conflict. Jiang acknowledges that many military strategists in China today still embrace a doctrine of a massive cyber first strike on US military and civilian targets, but argues these views have lost sway as China's strategic thinking and understanding of cyber capabilities has evolved (Jiang, 2019). Others concur with this assessment. For example, a former PLA colonel argues that China's 2015 Defense Paper reflects its decision to embrace a defensive cyber policy premised on assured retaliation (Jinghua, 2019). China appears, then, to have given up on the dream of a bolt-of-blue cyber-attack, recognizing the impracticality of such a concept.

However, the nature of this defensive posture may be more complex. According to Kevin Pollpeter, an American researcher viewed internationally as one of the foremost experts on China's military modernization, space, and cyber policy, the original logic of cyber warfare as an offensive tool still holds substantial sway over China's cyber doctrine. Specifically, based on an analysis of empirical cyber operations conducted by the PLA and authoritative primary sources, he alleges that China's military strategists uniformly believe in cyber warfare as a core component of modern warfare. In particular, China's cyber warfare doctrine emphasizes three cyber capabilities: exfiltrating data to derive intelligence benefits, limiting an adversary's options/slowing its responsiveness (by targeting logistical, communications, or commercial networks), and leveraging the asymmetric power of CFCCs as force multipliers. At the same time, the philosophy for cyber warfighting emphasizes the legitimacy of Chinese interests, use of first strikes and offensive actions, use of asymmetric weapons in order to counter America's conventional military superiority over the PLA, and a belief in cyber's potential for unlimited destruction. As a result, he concludes that China's cyber doctrine views cyber operations as operationally offensive, but its leadership at the strategic level views cyber weapons as inherently defensive – reconciling the evidence he finds with the "defensive" cyber narrative explained above (Pollpeter, 2015). Other research similarly finds that the offensive strategy persists despite China's supposed cyber pivot to a defensive position. This defensive doctrine still incorporates deep-hitting cyber strikes into military operations, including the specific targeting of command and control structures as part of an 'acupuncture warfare' defense that seeks to paralyze enemy militaries that have conventional superiority (Kanwal, 2009). China thus may claim to only use these weapons in retaliation or pre-emptive self-defense, but crisis scenarios specifically create the pressures to use such weapons upon such grounds.

One of the key reasons for this defensive mindset among strategic leadership is a notion of inferiority relative to the United States in the cyber realm. According to the same Chinese sources as cited before, China's investment in cyberspace derived from its concerns about

America's cyber evolution. Beyond the American head-start in development of cyber warfighting capabilities, China perceived a need to react given the US has a distinct advantage over China via supply chain interdiction: key Chinese network technologies and software and hardware come from the "eight King Kongs," or Qualcomm, IBM, Apple, Cisco, Google, Microsoft, Intel, and Oracle (Jinghua, 2019). Additionally, China's cyber efforts have placed substantial emphasis on policing content domestically through its so-called "Great Firewall." Given the resources dedicated to these activities, China has historically under-resourced efforts to build a defense against technical exploitation by foreign powers, suggesting a perceived or actual weakness in the cyber warfare realm (Lindsay, n.d.).

One piece of key evidence for this more aggressive mentality informing China's cyberwarfare doctrine is the writing of Major General Ye Zheng. Zheng's perspective is crucial – he is widely regarded as one of the earliest and most authoritative thinkers on cyberwarfare and his affiliation with the AMS Operational Theory and Regulations Research Department gives him tremendous influence over the creation of official PLA doctrine (Kania, 2016). Ye Zheng articulates a vision of cyber warfare that exemplifies a belief in its asymmetric power, going so far as to claim: "Just as nuclear warfare was the strategic choice of the industrial age, cyberwarfare is becoming the strategic go-to of the information age"(Zheng, n.d.). He further views all cyber weapons as falling into five categories – one being cyber defense, and the other four all being different offensive uses. Additionally, he advances a notion of strict cyber sovereignty, saying: "I would argue that invading a country in cyberspace is in essence the same as invading its lands, seas and oceans, skies and space, which are all considered violations of national sovereignty" (Zheng, n.d.). Such a claim illustrates a dangerous perception of cyberspace as a realm for confrontation, especially given its extremely porous nature. Thus, both his vocal belief in cyber weapons' unlimited, asymmetric power and his notions of cyberspace show how Zheng – and, probabilistically, Chinese cyber doctrine – conforms to Pollpeter's interpretation.

Another key concept in China's cyber doctrine is equivalence. This strategy, common to many cyber powers including the US, embraces a belief in a flexible response in which cyber-attacks can be met with kinetic responses of supposed equal weight. Notably, this strategy is the same that nuclear states have occasionally employed, threatening nuclear responses to conventional aggression, which some argue helped lead to the Cuban missile crisis. The opacity of China's cyber doctrine makes its equivalence policy increasingly destabilizing (Lieberthal & Singer, 2012). This logic further affirms the likelihood that a confrontation between China and another state would see the integrated deployment of CFCCs. At the same time, it also suggests that China could employ cyber operations in reaction to perceived aggressions in non-cyber realms. Ye Zheng's logic in particular illustrates how China's cyber doctrine deviates from traditional understandings of the nature of cyber operations. His emphasis on the targeting of non-military communications, transportation, and financial systems (analogous perhaps to Russia's cyber-attacks on Georgia in 2008) illustrates a receptiveness to the use of CVCCs that much US/Western literature has thus far dismissed. By blurring the distinctions between military and non-military targets, the Chinese cyber doctrine uniquely expands the scope of cyberwarfare. Conventional thinking about cyber weapons limits their value to direct integration into military operations; however, China's cyber doctrine extends beyond that application to see cyber weapons as having distinct political value as CVCCs demonstrate resolve and counter China's deficiencies such as its conventional military inferiority.

Finally, while China's cyber militia often captures the interest of China observers, this force is largely irrelevant for understanding the cyber-nuclear nexus. This militia – a fascinating manifestation of civil-military integration in a regime that traditionally seeks to centralize all military power – does not empirically influence military-to-military interactions. Because these groups target civilian cyberspace and lack any regular PLA chain of command, they have limited effectiveness in crisis scenarios (though their zealous nationalism is considered to introduce a degree of instability into the cyber realm more generally) (Sheldon & McReynolds, 2015).

Understanding Sino-US Conflict Escalation

While the odds of a conventional war, as well as subsequent nuclear escalation, between the US and China are unlikely, experts have recently dedicated increasing attention to the subject, given the consequences of such a scenario, recent intensification of security competition between the two powers, and the credibility of the logic of these assessments. In particular, those who envision escalation examine the potential for escalation given the interactivity between Chinese and American doctrines for conventional forces in the Pacific (Talmadge, 2017). China's strategy purportedly relies on anti-access, area denial (A2/AD) as a strategy to prevent American force projection into key maritime areas, including around Taiwan. In response, the US supposedly developed a strategy called AirSea Battle, using a combination of passive defenses and offensive action across domains including cyber, to disable China's capacity to enact A2/AD (Biddle & Oelrich, 2016). In 2015, the US renamed the concept, calling it the Joint Concept for Access and Maneuver in the Global Commons (JAM-GC).

Barry Posen's theory of Soviet nuclear escalation in the face of NATO conventional aggression serves as a critical foundation for the body of literature investigating the potential of nuclear escalation potential. His argument developed the idea that NATO's conventional warfighting doctrine would inadvertently threaten components critical to the USSR's assured retaliation, creating use-em-or-lose-em pressures on the USSR and thus causing catastrophic escalation as a result of miscalculation (Posen, 2014). In that spirit, many have applied a similar form of analysis regarding JAM-GC's potential to threaten critical Chinese assets such that it would feel pressured to surpass the nuclear threshold. Joshua Rovner's analysis suggests that, with US targeting of China's ballistic missiles, launchers, and infrastructure for targeting and guidance, Chinese officials may perceive such attacks as US attempts to neutralize the PLA's nuclear forces (Rovner, 2012). An in-depth analysis of military capabilities on both sides concludes A2/AD and JAM-GC will likely lead to contested battlespaces in the South and East China seas, with particular risk over Taiwan as China will feel increasingly able to prevent American access to the island in a crisis. As a result, the inability for either side to conclusively prevent a conflict will lead to mutual restraint or rapid escalation, with the latter more likely in the event of an unexpected crisis (Biddle & Oelrich, 2016).

More broadly, military planners on both sides of the Pacific may have overconfidence in their ability to manage crises, causing them to underestimate the degree of instability and potential for miscalculation in a conflict between the US and China. In particular, the potential for the US to unintentionally sink a Chinese SSBN during a conventional clash could trigger escalation (Goldstein, 2013).

Caitlin Talmadge makes a crucial addition to this body of literature. While analysis of military capabilities matters for these escalation scenarios, she rightly points out that the psychological reaction by Chinese leaders will play a key role in the potential for crisis spiraling. Viewing a military degraded by American actions, China's leaders will likely behave far less rationally than assumed, given the failure of previous beliefs in the supremacy of A2/AD and the deterrence capabilities of assured retaliation, as well as the fog of war. Under such conditions, Talmadge illustrates how Chinese leaders could perceive US actions as a conventional counterforce operation, with the destruction of nuclear ballistic missiles co-located with conventional ballistic missiles seen as the beginning of the destruction of the entire nuclear arsenal. As a result, PLA leaders may embrace a nuclear strike as a last best means of regaining a military advantage and/or as a coercive tool to deescalate. This development is psychological – it hinges on whether China's leadership perceives its forces have been degraded beyond a critical threshold for the nation's security (Talmadge, 2017).

Is this body of literature premised on a reasonable risk of crisis? Yes. The most alarming scenario concerns Taiwan. China's conventional military buildup suggests it is actively considering ways to re-take the island, a move which is intimately connected to CCP-style nationalism and Xi Jinping's emphasis on reunification by 2049, the 100-year anniversary of the founding of the PRC. However, such a situation could be triggered earlier should the Taiwanese independence movement make a particularly concerted effort at separating itself from China or should nationalist fervor or popular dissent within mainland China force the regime to act on Taiwan. General consensus suggests the PLA will not launch an all-out invasion of Taiwan, but rather will attempt to coerce Taiwan, which by nature will require the threat of A2/AD to deter the US from supporting Taiwan and thereby trigger a JAM-GC response (Biddle & Oelrich, 2016; Kastner, 2015; Talmadge, 2017). Additionally, the potential for an unintended clash at sea between US and Chinese naval vessels in the course of US freedom of navigation operations, presents the risk of crisis mismanagement that escalates to the enaction of A2/AD (Allison, 2017). While these conflict triggers are unlikely, they are still credible, and lend credibility to the literature attempting to understand the risk of nuclear escalation. More broadly, the empirical record suggests brinksmanship crises can occur with relative frequency between superpowers (e.g., Suez 1956, Berlin 1961, Cuba 1962, Czechoslovakia 1968, 1969 Sino-Soviet border crisis, Able Archer crisis 1983).

While the literature on the nuclear risk in the Sino-American relationship has grown increasingly nuanced in recent years, it has thus far given only cursory attention to cyber warfare. Interestingly, cyber warfare alters both the conventional military factors and the psychological factors that influence escalation to, and at, the level of a brinksmanship crisis.

Both of the explanations for the cyber-nuclear nexus map well to the China-specific nuclear escalation literature. The cyber fog of war theory directly bolsters Talmadge's argument for escalation to such a crisis, as compromised NC3 or BMC3 would greatly exacerbate the fog-of-war effects she describes in her escalation scenario. OCOs compromising communications systems would push PLA leadership to believe it were losing its ability to understand what was happening across the battlefield. OCOs compromising weapons systems would push PLA leadership to believe it were losing its ability to wield its most crucial weapons. In both cases, it would immediately view the US's kinetic operations in a more alarmist light. The nature of CFCC's as force multipliers is critical – their ability to augment the influence of kinetic operations, in addition to severing critical communications, complicates level-headed analysis of military operations.

To delve to a deeper level of specificity in this scenario, consideration of the effect of cyberwarfare on a scenario involving the employment A2/AD and JAM-GC demonstrates the risk cyber poses. JAM-GC seeks to deny China's ability to execute A2/AD, which necessitates targeting of conventional command and control systems, conventional ballistic missile launchers, and early detection radar systems. CFCCs would almost assuredly be integrated into this operation. However, China co-mingles its conventional and nuclear command and control, and its long-range radars that would be used for targeting American targets as part of its A2/AD strategy also serve as a nuclear early-warning system (Twomey, 2011). A cyber-attack aimed at denying China's ability to execute A2/AD would therefore risk creating fears of a US nuclear counterforce operation. This co-mingling by China could be a deliberate strategy – by intentionally making attacks on these systems more dangerous, China could be leveraging the risk of instability to deter US attacks on its BMC3. However, this strategy predicates on an assumption of perfect rationality that would be challenged in a crisis scenario, and JAM-GC reflects a strategy of targeting China's BMC3 that does not seem to take concern over the co-mingling problem. Admittedly, this strategy itself could be a US attempt to deter China from ever invoking A2/AD, on the same principle of purposefully leveraging the risk of greater instability. This trend reveals the paradox of interactivity between nuclear and cyber weapons, with the former perhaps providing a deterrent to use of the latter; more on this effect will be discussed at the end of this section. However, to dismiss the possibility of China employing A2/AD and the US responding with JAM-GC ignores the genuine risks of crises such as the Taiwan scenario. Additionally, China uses the same transmitters to communicate with its SSBNs and SSNs; in a JAM-GC scenario, the US would almost certainly compromise these transmitters using cyber means, which would have the side effect of severing communication between PLA leadership and the sea-based leg of its nuclear triad (Talmadge, 2017). Such actions directly contribute to the psychological breakdown Talmadge's scenario describes.

Conversely, China's execution of A2/AD would similarly introduce escalatory risk via cyber operations. US satellites positioned over Taiwan, for example, would provide crucial information for precision strikes; as such, a key aspect of enacting A2/AD would be the elimination of these tools, given the satellite's crucial role in guiding battlefield operations (some analysts have even suggested Chinese leaders see these satellites as a "Clausewitzian center of gravity") (Bahney et al., n.d.; Biddle & Oelrich, 2016). Chinese leaders may wish to avoid a hard ASAT, opting instead for a cyberattack; nevertheless, such actions are particularly destabilizing. These US satellites are a crucial part of the NC3 system, serving as early warning systems; US military planners would very likely interpret the incapacitation of one of these satellites by the PLA as the opening move of a broader war, forcing an escalatory response.

Beyond the fog of war scenario, the nuclear balance of power theory for the cyber-nuclear nexus applies to US-China crisis scenarios. In this case, the theory suggests that in the conditions of a brinksmanship escalation between the US and China, the US may embrace more aggressive behavior than these scenarios assume. As explained earlier, the nations with the most resources and experience hold far greater cyber arsenals than the rest of the world, presumptively making the US the world's greatest cyber superpower. Additionally, China's nuclear doctrine calls for a limited form of assured retaliation, embracing a nuclear arsenal of only a few hundred weapons (Narang, 2014). This posture greatly enhances the risk to China's nuclear arsenal posed by cyber operations, because as arsenal sizes become smaller, the likelihood of a coordinated cyber-attack achieving disarming capacity dramatically increases (S. J. Cimbala, 2017). The relative power imbalance between the US and China incentivizes the US, as the stronger cyber power, to prepare a debilitating cyberattack as an insurance policy against the weaker power should deterrence fail (Gartzke & Lindsay, 2017. 45). The US would thus hold both incentive and capability to prepare OCOs that undermine or incapacitate China's nuclear arsenal. that secretly upset the nuclear balance of power in a brinksmanship crisis between China and the US. By holding this hidden weapon, the US could secretly hold a strategic advantage, creating a form of deterrence failure during a brinksmanship crisis as the accepted level of risk by both sides that far surpasses that which they would accept if both sides understood the true balance of power.

The additional scenarios deriving from the balance of power scenario also apply. Should the US recognize its capabilities advantage and prepare a debilitating cyber operation as a form of insurance policy, China – still a well-resourced, highly capable cyber power – would stand a chance of detecting the intrusion. As a result, it could believe the US were preparing a counterforce strike and instantly begin reading the crisis in a much more hostile frame, embracing the same psychological mindset Talmadge warns against. This interpretation is more likely given the historical evolution of China's cyberwarfare doctrine, which has painted China as catching up to the dangerously superior US. The scenario would become even worse if China were unable to remedy the cyber intrusion, meaning it would face stark use-em-or-lose-em incentives.

In addition to these two main scenarios for cyber-nuclear nexus, some aspects of China's cyberwar fighting doctrine introduce destabilizing elements to crisis management. Given the importance China places on cyber control of its people and its belief in preserving domestic stability to ensure regime survival above all else, it is likely to view US cyber operations that compromise facets of its network-based system of control in a far more alarmist light than what the US might anticipate. As a result, US operators who have been given authority to conduct OCOs by NSPM 13 may launch operations they perceive to reside in the realm of low-intensity conflict, but which CCP leaders could interpret as a dramatic step up the escalation ladder. More broadly, this lack of consensus for where specific OCOs exist on the escalation ladder may lead to inadvertent escalation.

At the same time, China's belief in cyber warfare's balance-of-power-altering potential and its sufficient resources and capabilities suggest it likely may develop significant capabilities to undermine the US NC3. China's deployment of such tools would square with its "defensive" cyber doctrine, viewing the development of such tools as an insurance policy similarly to how the US would. Under the balance of power theory of cyber-nuclear nexus, this advantage may embolden China in a brinksmanship crisis, leading to improper risk taking. The US also stands a good chance of detecting the intrusion, which would create the same psychological danger as would China's detection of a US intrusion. Though China's leadership would likely view intrusions into US BMC3/NC3 as defensive in nature, as Pollpeter explains – perhaps justified to themselves as for the purpose of intelligence – the US would view such an intrusion as the PLA laying groundwork for an attack under the principle of capabilities-based assessments.

Additionally, China's beliefs about cyber warfare imply it could use cyber to escalate in response to a detected intrusion or a kinetic operation by the US. China's cyber warfare doctrine emphasizes cyber weapons as weapons of unlimited potential, serving as great equalizers in situations in which the balance of power disfavors the PLA. As a result, should China react to US conventional moves with a massive array of integrated cyber-attacks (rather than nuclear escalation, as is sometimes assumed in the literature), the compromise of US NC3, BMC3, or missile launch systems would likely pressure the US to nuclear use or a substantial conventional retaliation. In these cases, cyber adds more steps to the escalation ladder, but also makes it easier to begin moving up the ladder unintentionally, therefore enhancing the risk of escalation beyond cyber.

The literature on the nature of cyberwarfare unfortunately assumes that all countries think primarily in terms of CFCCs. As discussed in the previous section, China's cyber doctrine seems to embrace an idea of cyber operations in an almost total-war mindset, suggesting the use of CVCCs. In a crisis scenario, a CVCC could be a uniquely attractive option to Chinese leadership, who understand their conventional inferiority but wish to demonstrate a strong resolve and show of force to the United States as a deterrence strategy. As mentioned earlier, it is not clear whether or not CVCCs in the present have significant destructive/disruptive capacity, though as 5G and an informatized economy develop, this capacity could come into existence. Such a move by the PLA, however, could backfire. The United States has a culture of extremely strong reactions to attacks on its homeland, from 9/11 to Pearl Harbor to the beginning of the Mexican-American war. As such, the US could reasonably react to a debilitating Chinese attack on the nation's electric grid or the data infrastructure undergirding the core of the future economy with saber-rattling or an actual counter rather than backing down as the Chinese intended.

In each of these scenarios, cyberwarfare leads to misunderstandings or miscalibration as the US and China seek to navigate the difficult task of sending signals and interpreting responses in escalation to and management of a brinksmanship crisis. Admittedly, nuclear weapons are weapons of compellence, meaning one of their effects is to prevent unstable scenarios from escalating. The cyber-nuclear nexus thus exists in a state of paradox: one half of the equation destabilizes and escalates, while the other half stabilizes and de-escalates. This confusion underscores the need for better understandings of the effects both kinds of weapons have on escalation pathways. Reasonably, both effects will likely influence nuclear crisis. However, while this makes precisely and accurately measuring the extent to which cyber aggression leads to escalation difficult, the escalatory effects considered in this paper illustrate that these effects bolster the view of escalation pessimists observing the US-China relationship.

Conclusion

The secrecy surrounding cyberweapons, the uncertainty over their exact technical capabilities, and the dilemmas in understanding China's cyber doctrine all underscore both the ambiguity inherent to assessments of the cyber-nuclear nexus and the importance of understanding such a risk. Cyber weapons pose a distinct, often underappreciated threat as military leaders integrate OCOs into broader operations, augmenting the impact of military operations in ways they may not fully grasp. These operations, especially during crisis scenarios, may upset traditional assumptions about nuclear stability. Both because of their ability to induce a fog of war and because of their ability to secretly alter the balance of power in a nuclear dyad such that risk-taking is not properly bounded, cyber weapons create a legitimate threat of a cyber-nuclear nexus.

The cyber-nuclear nexus lends credibility to the body of literature weighing the possibility of nuclear escalation between the US and China. Should a crisis occur over Taiwan or an accidental clash in the East or South China Seas, China's doctrine of A2/AD and the US's JAM-GC response would likely integrate cyber operations in ways that would further destabilize the conflict. In these scenarios, JAM-GC CFCCs could significantly contribute to the fog of war and Chinese leaders' perceptions of an oncoming counterforce strike. Additionally, these capabilities could embolden US leaders due to their secret advantage, leading to unsustainable risk-taking as each side escalates from the initial crisis point. Conversely, China's cyber doctrine suggests it would employ CFCCs early on in an A2/AD scenario, and such actions could contribute to similar fog of war dilemmas for the American side. Such actions would also dramatically escalate any initial conflict, especially should they target US satellites in the region that serve as a crucial node of the NC3 system. Should either side detect a cyber compromise in its NC3, it would perceive the other side as dangerously hostile while at the same time facing strong use-lose pressures. Finally, a higher appetite for offensive action in the cyber realm on both sides of the Pacific and potential Chinese considerations of CVCCs illustrate how these nation's cyberwar doctrines may unintentionally cause conflicts in other realms to spiral to the nuclear level.

These gamed-out scenarios, based on analysis of technical cyber capabilities, general theories of the cyber-nuclear nexus, and implications of China's cyberwarfare doctrine and A2/AD strategy, further support the view of the "escalation pessimists" watching the US-China relationship. If the risk of this cyber-nuclear nexus is legitimate, conflict resolution will likely be more complex than in the pre-cyber warfare age. Such a risk implies the need for stronger cyber norms, potential limitations on cyber weapons, and, perhaps chiefly of all, more transparency in cyber warfighting doctrine. However, given both strong emphasis on the secrecy of weapons and the technical nature of cyber weapons, these measures will be extremely difficult to enact, suggesting perhaps the most fruitful pathway forward is stronger Sino-American military-to-military relations that could better communicate cyber doctrines and build better understanding in order to avoid catastrophic, miscalculated escalation when crises do occur.

This paper raises a variety of questions for future research. Given the ambiguity surrounding cyber weapons, understanding both what OCO capabilities look like and the sorts of vulnerabilities in NC3, BMC3, and weapons systems will add far more precision to any understanding of the cyber-nuclear nexus. Additionally, understandings of China's cyber warfighting doctrine are difficult, and particularly given that China may have only developed a firm understanding of its doctrine within the last 2-3 years underscores the need for more research in this area. Another critical area of research is understanding the extent to which military commanders view the interactive effects between cyber warfighting and conventional warfighting, given the importance of escalation management that OCOs will complicate.

This cyber-nuclear nexus also adds an important twist to an ongoing debate relating to nuclear stability. One school of thought suggests that the risk of nuclear escalation provides a useful deterrent on conventional confrontation. In the taken case of A2/AD and JAM-GC, followers of this thinking suggest the destabilizing risk that JAM-GC introduces will deter China from engaging in A2/AD. Conversely, others argue this escalatory risk is bad, as attempting to leverage nuclear instability to derive some conventional military advantage simply takes on too much existential risk. Future research should incorporate an understanding of cyber warfare's destabilizing influence on this debate. This research could investigate whether or not the risk of instability derived from cyber operations is sufficiently perceived, which would indicate the validity of using the threat of CFCCs in a conflict as a way to deter conventional military engagement in the first place. Additionally, it could investigate the extent to which countries' weaknesses to cyber weapons in their critical military infrastructure (for example, China's co-mingling of its NC3 and BMC3) is intentional as a strategic choice to prevent attacks from an adversary.

References

Allison, G. (2017). How America and China Could Stumble to War. *The National Interest*. https://nationalinterest.org/feature/how-america-china-could-stumble-war-20150.

Bahney, B. W., Pearl, J., & Markey, M. (n.d.). Antisatellite Weapons and the Growing Instability of Deterrence. In Eric Gartzke & J. Lindsay (Eds.), *Cross-Domain Deterrence: Strategy in an Era of Complexity*. Oxford University Press. Retrieved May 4, 2020, from https://www-oxfordscholarship-com.ezp-prod1.hul.harvard.edu/view/10.1093/oso/9780190908645.001.0001/oso-9780190908645-chapter-6

Biddle, S., & Oelrich, I. (2016). Future Warfare in the Western Pacific: Chinese Antiaccess/Area Denial, U.S. AirSea Battle, and Command of the Commons in East Asia. *International Security*, *41*(1), 7–48.

Borghard, E. D., & Lonergan, S. W. (2019). Cyber Operations as Imperfect Tools of Escalation. *Strategic Studies Quarterly*, *13*(3), 122–145. JSTOR.

Cimbala, D. S. J. (2016). Nuclear Deterrence in Cyber-ia: Challenges and Controversies. *Air & Space Power Journal*, *30*(3), 54–63.

Cimbala, S. J. (2017). Nuclear deterrence and cyber warfare: Coexistence or competition? *Defense & Security Analysis*, *33*(3), 193–208. https://doi.org/10.1080/14751798.2017.1351142

Defense Intelligence Agency. (2019). *China Military Power* (DIA-02-1706-085). https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/China_Military_Power_FINAL_5MB_20190103.pdf

Department of Defense. (2018). *Summary: Department of Defense Cyber Strategy 2018* (p. 10). https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF

Dougherty, R. (1987). The Psychological Climate of Nuclear Command. In *Managing Nuclear Operations* (pp. 407–425). The Brookings Institution.

Gartzke, Erik, & Lindsay, J. R. (2017). Thermonuclear cyberwar. *Journal of Cybersecurity*, *3*(1), 37–48. https://doi.org/10.1093/cybsec/tyw017

Goldstein, A. (2013). First Things First: The Pressing Danger of Crisis Instability in U.S.-China Relations. *International Security*, *37*(4), 49–89. JSTOR.

Grigsby, A. (2017, June 22). Canada's Military Gets More Cyber, and the Headaches That Come With It. *Council on Foreign Relations*. https://www.cfr.org/blog/canadas-military-gets-more-cyber-and-headaches-come-it

Herpig, S. (2018, September 4). As Germany Moves Toward a More Offensive Posture in Cyberspace, It Will Need a Vulnerability Equities Process. *Council on Foreign Relations*. https://www.cfr.org/blog/germany-moves-toward-more-offensive-posture-cyberspace-it-will-need-vulnerability-equities

Horowitz, M., Kania, E., Allen, G., & Scharre, P. (2018). *Strategic Competition in an Era of Artificial Intelligence*. Center for a New American Security. https://www.cnas.org/publications/reports/strategic-competition-in-an-era-of-artificial-intelligence

Jiang, T. (2019). From Offense Dominance to Deterrence: China's Evolving Strategic Thinking on Cyberwar. *Chinese Journal of International Review*, *01*(02). https://doi.org/10.1142/S2630531319500021

Jinghua, L. (2019, April 1). What Are China's Cyber Capabilities and Intentions? *International Peace Institute Global Observatory*. https://theglobalobservatory.org/2019/03/what-are-chinas-cyber-capabilities-intentions/.

Kania, E. (2016). A Force for Cyber Anarchy or Cyber Order? —PLA Perspectives on 'Cyber Rules.' *Jamestown*, *16*(11). https://jamestown.org/program/a-force-for-cyber-anarchy-or-cyber-order-pla-perspectives-on-cyber-rules/

Kanwal, G. (2009). China's Emerging Cyber War Doctrine. *Journal of Defence Studies*, *3*(3).

Kastner, S. L. (2015). Is the Taiwan Strait Still a Flash Point?: Rethinking the Prospects for Armed Conflict between China and Taiwan. *International Security*, *40*(3), 54–92.

Kehler, Robert C. (2013). *HEARING TO RECEIVE TESTIMONY ON U.S. STRATEGIC COMMAND AND U.S. CYBER COMMAND IN REVIEW OF THE DEFENSE AUTHORIZATION REQUEST FOR FISCAL YEAR 2014 AND THE FUTURE YEARS DEFENSE PROGRAM*. https://www.armed-services.senate.gov/imo/media/doc/13-09%20-%203-12-13.pdf

Lieberthal, K., & Singer, P. W. (2012). *Cybersecurity and U.S.-China Relations* (p. 52). 21st Century Defense Initiative and John L. Thornton China Center at Brookings. https://www.brookings.edu/wp-content/uploads/2016/06/0223_cybersecurity_china_us_lieberthal_singer_pdf_english.pdf

Lindsay, J. R. (n.d.). Introduction. In J. R. Lindsay, T. M. Cheung, & D. Reveron (Eds.), *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*. Oxford University Press. Retrieved April 17, 2020, from https://www-oxfordscholarship-com.ezp-prod1.hul.harvard.edu/view/10.1093/acprof:oso/9780190201265.001.0001/acprof-9780190201265-chapter-1

Long, A., & Green, B. R. (2015). Stalking the Secure Second Strike: Intelligence, Counterforce, and Nuclear Strategy. *Journal of Strategic Studies*, *38*(1–2), 38–73. https://doi.org/10.1080/01402390.2014.958150

Mussington, D. (n.d.). Strategic Stability, Cyber Operations and International Security. *Centre for International Governance Innovation*. Retrieved April 21, 2020, from https://www.cigionline.org/articles/strategic-stability-cyber-operations-and-international-security.

Nakashima, E. (2018, September 20). White House authorizes 'offensive cyber operations' to deter foreign adversaries. *Washington Post*. https://www.washingtonpost.com/world/national-security/trump-authorizes-offensive-cyber-operations-to-deter-foreign-adversaries-bolton-says/2018/09/20/b5880578-bd0b-11e8-b7d2-0773aa1e33da_story.html.

Narang, V. (2014). China. In *Nuclear Strategy in the Modern Era: Regional Powers and International Conflict*. Princeton University Press.

Pollpeter, K. (2015). Chinese Writings on Cyberwarfare and Coercion. In J. R. Lindsay, T. M. Cheung, & D. Reveron (Eds.), *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*. Oxford University Press. https://www-oxfordscholarship-com.ezp-prod1.hul.harvard.edu/view/10.1093/acprof:oso/9780190201265.001.0001/acprof-9780190201265-chapter-6

Porche III, I., Paul, C., Serena, C., Clarke, C., Johnson, E.-E., & Herrick, D. (2017). *Tactical Cyber: Building a Strategy for Cyber Support to Corps and Below*. RAND Corporation. https://www.rand.org/content/dam/rand/pubs/research_reports/RR1600/RR1600/RAND_RR1600.pdf

Posen, B. R. (2014). *Inadvertent Escalation: Conventional War and Nuclear Risks*. Cornell University Press. http://ebookcentral.proquest.com/lib/harvard-trial/detail.action?docID=3138481

Rovner, J. (2012). AirSea Battle and Escalation Risks. *SITC-NWC 2012 POlicy Briefs*, *2012*(Policy Brief 12). https://escholarship.org/uc/item/08m367zt

Rudesill, D. (2018, August 29). Trump's Secret Order on Pulling the Cyber Trigger. *Lawfare*. https://www.lawfareblog.com/trumps-secret-order-pulling-cyber-trigger

Sheldon, R., & McReynolds, J. (2015). Civil-Military Integration and Cybersecurity: A Study of Chinese Information Warfare Militias. In J. R. Lindsay, T. M. Cheung, & D. Reveron (Eds.), *Civil-Military Integration and Cybersecurity: A Study of Chinese Information Warfare Militias*. Oxford University Press.

https://www-oxfordscholarship-com.ezp-prod1.hul.harvard.edu/view/10.1093/acprof:oso/9780190201265.001.0001/acprof-9780190201265-chapter-8

Smeets, M. (2018). The Strategic Promise of Offensive Cyber Operations. *Strategic Studies Quarterly*, *12*(3), 90–113.

Stephan, P. B. (2020). *Big Data and the Future Law of Armed Conflict in Cyberspace* (SSRN Scholarly Paper ID 3521387). Social Science Research Network. https://papers.ssrn.com/abstract=352138.

Talmadge, C. (2017). Would China Go Nuclear?: Assessing the Risk of Chinese Nuclear Escalation in a Conventional War with the United States. *International Security*, *41*(4), 50–92.

Twomey, C. P. (2011). Asia's Complex Strategic Environment: Nuclear Multipolarity and Other Dangers. *Asia Policy*, *11*, 51–78. JSTOR.

US Government Accountability Office. (2015). *Nuclear Command, Control, and Communications: Update on DOD's Modernization* (GAO-15-584R). https://www.gao.gov/products/GAO-15-584R

US Joint Chiefs of Staff (1982). *A Historical Study of Strategic Connectivity, 1950-1981*. https://nsarchive2.gwu.edu/nukevault/ebb403/docs/Doc%201%20-%20connectivity%20study%201982.pdf

Wasson, J. T., & Bluesteen, C. E. (2018). Taking the Archers for Granted: Emerging Threats to Nuclear Weapon Delivery Systems. *Defence Studies*, *18*(4), 433–453. https://doi.org/10.1080/14702436.2018.1528137

White House. (2018). *National Cyber Strategy of the United States of America*. https://apps.washingtonpost.com/g/documents/world/trump-administrations-national-cyber-strategy/3212/

Zheng, Y. (n.d.). From Cyberwarfare to Cybersecurity in the Asia-Pacific and Beyond. In J. Lindsay, T. M. Cheung, & D. Reveron (Eds.), & Y. Fan (Trans.), *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*. Oxford University Press. Retrieved April 19, 2020, from https://www-oxfordscholarship-com.ezp-prod1.hul.harvard.edu/view/10.1093/acprof:oso/9780190201265.001.0001/acprof-9780190201265-chapter-5