Cyber Offense and a Changing Strategic Paradigm

Leonard Spector

To cite this article: Leonard Spector (2022) Cyber Offense and a Changing Strategic Paradigm, The Washington Quarterly, 45:1, 38-56, DOI: 10.1080/0163660X.2022.2054123

To link to this article: https://doi.org/10.1080/0163660X.2022.2054123

Published online: 25 Apr 2022.
Although much secrecy surrounds the issue, unclassified literature provides numerous indications that China, Russia, and the United States are pursuing two offensive cyber capabilities with the potential to alter strategic relations among these countries. The two capabilities take the form of different modes of stealthily implanted malware to be used, as needed, in a future military crisis. One of these cyber capabilities is designed to compromise one or more elements of an adversary’s nuclear weapon systems—including nuclear command, control, communications, and early warning capabilities—and/or to disable an adversary’s nuclear weapons and delivery systems themselves by tampering with supply chains for internal electronic components or in-weapon computer code.1 The second cyber effort is intended to disrupt, perhaps catastrophically, an adversary’s critical infrastructure—i.e. its electric power, transportation, financial, communications, and other key systems.2

Many in the national security community fear that such cyber operations carry the potential for dangerous, unpredictable consequences. High on the list of concerns is that offensive cyber tools intended for use against nuclear weapon systems will create uncertainties in potential target countries regarding the integrity of their second-strike nuclear forces. This, it is feared, could create incentives to
strike first in a crisis, eroding strategic stability based on certainty of devastat-
ing retaliation in kind to a nuclear attack. A related oft-noted worry is that an
adversary’s or non-state actor’s cyber tampering with a state’s early warning
systems could lead the latter to launch its nuclear forces based on spurious
information indicating it was under attack, or on the erroneous assumption
that the tampering, which may have in fact been undertaken only to collect
intelligence or to interfere with conventional military operations, was precur-
sor to such an attack.3 In the case of a cyberattack against a state’s critical
infrastructure, a leading concern is that the state’s response to such attacks
cannot be known in advance, but could set in motion a volatile escalatory
spiral, leading to conventional conflict and ultimately possible resort to
nuclear arms.4

Without minimizing these challenges, however, there appears to be far more at
issue in this evolving situation. Specifically, it appears that when taken together,
cyber operations against nuclear weapon systems, which introduce uncertainties
regarding the performance of such systems, and cyber operations against critical
infrastructure, which introduce potent sub-nuclear offensive capabilities, are
slowly moving nuclear arms somewhat further into the background in future
great power confrontations. At the same time, threatened or actual use of destruc-
tive counter-critical-infrastructure cyberattacks appears to be moving more
toward the forefront in such situations. In effect, although nuclear arms will
undoubtedly remain an ever-present dimension of China-US and Russia-US
relations as would-be guarantors of national survival, these antagonists will
have increasing reason in their clash of wills to hold nuclear weapons in
reserve, while giving cyber attacks against critical infrastructure—subject to
fewer legal, humanitarian, and political restraints—a more prominent, direct,
and immediate role.5

This reorientation might seem a positive development by possibly lowering the
threat of nuclear conflict. But this optimistic conclusion is not clear-cut. To be
sure, the destruction from massive cyberattacks against critical infrastructure
would be orders of magnitude less than that caused by nuclear war. It is also
truethatcalibratedinfrastructurecyberattacksprovideadditionalpre-nuclear
rungs to the escalation ladder, possibly making resort to nuclear arms more
remote.6 Massive infrastructure cyberattacks, however, could nonetheless cause
catastrophic devastation, leading to years of national hardship and considerable
loss of life from the collapse of food, water, medical, and other essential systems.7
Moreover, the very fact that such infrastructure attacks avoid the unbounded cat-
calyzmofnuclearwariaincreasethelikelihoodthatthiscybercapabilitycouldbe
used, potentially to the great harm of the targeted state. Nor can the threat of
retaliation with nuclear arms to an unrestrained cyberattack be ruled out, a possi-
bility the United States, at least, appeared to invoke in the US 2018 Nuclear
Posture Review. China and Russia have also implicitly left the door open to responding with nuclear weapons to such an attack.

The potential readjustment of the roles of nuclear and cyber operations is rarely acknowledged or openly discussed in official pronouncements. Nonetheless, this shift appears to be the logical consequence of ongoing trends that, on one hand, cast a certain shadow over a number of nuclear-use options, while on the other, underline the increasing utility and usability of cyber assaults against critical infrastructure. Indeed, as this article went to press, initial developments in the conflict between Russia and Ukraine reflected the complex relationships introduced by cyber operations in a clash involving major powers. Importantly, the United States dismissed Russian President Vladimir Putin’s placing of his country’s nuclear forces on alert as empty posturing, but appeared to take the threat of Russian cyberattacks against US critical infrastructure more seriously, leading Washington to refrain from making such cyber strikes against Russia for fear of retaliation in kind.

These trends are discussed below, but first, several building blocks regarding cyber operations in these contexts need to be put in place. As will be seen later in this analysis, these postulates—the reciprocity of cyber threats; the limits of defenses; uncertainty as to the impairment of one’s nuclear weapon systems and critical infrastructure; uncertainty as to the efficacy of one’s offensive cyber intrusions; and the strategic dimensions of infrastructure attacks—are pervasive features of the cyber-infused international security landscape.

Cyber Building Blocks

As noted at the opening of this article, there are many indications that each side of China-US and Russia-US relationships is engaged in developing offensive cyber tools to compromise the other side’s nuclear weapon systems and critical infrastructure. (In this article “cyberattack,” “cyber strike,” and “cyber assault” are being used to denote the actual use of implanted malware to interfere with an adversary's activities, while “cyber intrusion,” “cyber efforts,” and “offensive cyber operations,” are used to denote the implanting of that malware, which is to remain dormant and, by definition, undetected until the time of use.) This means that, as the major nuclear powers attempt to advance these high-impact cyber threats against their opponents through stealthy malware, they must...
simultaneously recognize that they are, themselves, subject to the very same stealthy cyber threats. In effect, the cyber threat among these three powers is reciprocal but unverifiable. (Although this article focuses on China-US and Russia-US cyber activities to simplify the discussion, other nuclear-armed states also appear to be pursuing counter-nuclear-weapon-system (CNWS) and counter-critical-infrastructure (CCI) cyber operations. Many of the principles discussed here as applicable to the three leading nuclear powers would in many respects also apply in the case of other nuclear-armed dyads.)

It is also widely accepted that airtight defenses against such offensive cyber efforts are not possible. Moreover, it is generally believed that the increasing complexity of newer nuclear weapon systems and their associated software makes them more vulnerable to cyber disruption than older ones. The same holds true for critical infrastructure, as management of those systems relies increasingly on advanced digital controls. This means that each of the states at issue here must recognize that its nuclear weapon systems and critical infrastructure are currently vulnerable to cyber sabotage and will remain so going forward. Because the opponent’s cyber intrusions are intended to be undetectable, however, none of these states can know with confidence how badly or in what respect its nuclear assets and critical infrastructure may be at risk of disruption in a future confrontation.

At the same time, because no side can test its CNWS-malware under realistic conditions, no side can know how effective this malware may be, or whether its adversary may have silently detected and disabled it. The same holds true for testing national-scale CCI-cyber strikes, although it is possible to test such operations on a smaller scale, as seen for example in Russia’s partial shutdown of the Ukrainian electric power grid causing short-term blackouts in 2015 and 2016; the November 2020 Mumbai blackout that some Indian observers attribute to China; and the multiple 2021 ransomware attacks against US entities by Russia-linked hacking groups.

Finally, it needs to be recognized that because massive CCI-cyberattacks are seen as able to cause grave harm to the adversary’s homeland—harm of potential strategic consequence—these weapons, while far less destructive, share important characteristics with nuclear-armed intercontinental-range missiles. The degree of potential destructiveness from massive CCI-cyberattacks is the subject of continuing debate. There is widespread agreement that such attacks could not rival the devastation caused by nuclear weapons, but a preponderance of analysts holds that the damage caused could nonetheless be “catastrophic.” This has led some analysts to imagine that such cyberattacks could hypothetically serve as a
supplemental second-strike capability, combining in and reinforcing a retaliatory attack that employed a state’s surviving nuclear weapon assets or, in extremis, serving as the sole retaliatory mechanism.

Such CCI-cyber capability, in the form of stealthy malware, would by definition be hidden and would likely rely on installations and personnel separate from those associated with nuclear weapon operations; indeed, the massive retaliatory CCI-strike could be launched by operatives located anywhere in the world. In addition, it appears to be accepted that it is not possible to eradicate an adversary’s CCI-cyber capabilities preemptively. These factors would help make this capability secure and survivable after a nuclear attack on a state’s homeland, although like nuclear-armed submarines and mobile missiles, the malware would always be at risk of discovery and adversary countermeasures.

Cyber Shadow over Nuclear Weapons Systems

If the states in the China-US or Russia-US nuclear dyads believe that their respective strategic nuclear deterrents are subject to an adversary’s ongoing undetectable cyber intrusions, it follows that this situation must create at least a kernel of doubt among both opposing states’ decisionmakers as to the reliability of their respective nuclear weapon systems, doubt that can never be fully dispelled. This would seem to reduce both states’ incentives to be the first to launch its strategic nuclear forces in a crisis.

A related inhibition to striking first is that the would-be attacker must recognize that its opponent, in the course of infiltrating the would-be attacker’s nuclear systems, must have acquired an intimate understanding of the would-be attacker’s nuclear operations and the ability to monitor those operations so that the intruder could determine when a threat is emerging that calls for exploiting its dormant disabling cyber penetration. This provides a form of reciprocal non-consensual transparency, somewhat like that provided by satellite imagery, that taken together with other intelligence sources, would enable the intended target of the first strike to take pre-attack defensive measures, in particular activating its dormant CNWS-malware, and if warning time allowed, dispersing additional nuclear-armed assets, such as submarines to sea, or even launching a preemptive nuclear attack of its own.

If the adversary’s previously embedded cyber intrusions crippled the nuclear forces of the would-be first-strike state, it could leave the adversary’s retaliatory nuclear forces largely intact. Such thinking would make the idea of attacking first even less attractive than in the past when the attacking state could have had greater hopes of eliminating much of its adversary’s retaliatory capability. To be sure, the state contemplating the first strike might imagine that its
CNWS-cyberattacks could be launched as part of its initial onslaught to disrupt the target state’s retaliatory assets, but as noted, with no way to test the effectiveness of such cyberattacks, it is not clear how much added confidence the would-be attacker would gain.\textsuperscript{20}

Finally, as suggested above, the would-be attacker must also be concerned that even if its first strike largely destroyed the opponent’s nuclear retaliatory forces, the strike would likely leave intact the opponent’s ability to mount a massive retaliatory CCI-cyberattack against the first-strike nuclear attacker. Though hardly equal in potency to retaliation with nuclear arms, the latent threat to critical infrastructure would be difficult for decisionmakers in the would-be attacking state to ignore as they weighed the pros and cons of striking first.

As a corollary, if both states in either of the dyads recognize that their first-strike forces are at risk of compromise, they must also recognize that their respective second-strike nuclear forces are also under threat of cyber disruption. As analysts James Miller and Richard Fontaine have pointed out, this should make both states more cautious in future crises before engaging in behavior that might trigger an escalatory nuclear strike by the adversary to which the state subject to the nuclear attack might not be able to respond effectively in kind.\textsuperscript{21} Like first-strike uncertainty, this added caution impelled by second-strike uncertainty may also reduce the likelihood of nuclear weapon use when compared to the pre-cyber era. While it was noted in the introduction that some argue that a state’s concerns regarding its second-strike capabilities might induce it to strike first, as suggested here, the argument is circular. If a state must fear its second-strike assets (by definition the state’s most secure nuclear forces) are at risk of compromise, it must fear even more that its less well-protected first-strike assets are also at risk of sabotage, hardly an inducement to go first.\textsuperscript{22}

Prominent national security specialists Richard Danzig, writing in 2014, and Miller and Fontaine, in 2018, have said that in these conditions the traditional bedrock of strategic stability—mutually assured destruction (MAD)—would no longer apply, but the new state of affairs—mutually unassured or uncertain destruction (MUD)—could still be able to sustain strategic stability, albeit on different terms than in the past (as examined further below).\textsuperscript{23}

As seemingly unavoidable as the above considerations may be, for understandable reasons their full implications are rarely, if ever, directly confronted or even acknowledged in official pronouncements. Indeed, judging by the eagerness with which China, Russia, and the United States are modernizing their nuclear forces,
these three states give the appearance of having little concern regarding the cyber sabotage threat. These governments, however, would hardly want to admit that they are aggressively pursuing cyber mechanisms to compromise the nuclear weapon systems of their adversaries, much less acknowledge that they believe their own systems may currently be impaired by an adversary’s cyber intrusions.

Official postures aside, in the United States, at least, there are clear indications of apprehension. The 2018 Nuclear Posture Review, for example, although it does not acknowledge that US nuclear systems may already be penetrated, declares that Chinese and Russian cyber activities are seeking to interfere with US nuclear command, control, and communication systems and that the United States will strengthen protection against such threats. The implication, if adversaries are probing and cybersecurity needs strengthening, is that US nuclear weapon systems, to a greater or lesser degree, are currently vulnerable to potentially dangerous cyber intrusions. Similarly, by requiring the Department of Defense to examine all major US weapons systems for cyber vulnerabilities and take steps to mitigate such weaknesses, the US National Defense Authorization Act (NDAA) for fiscal year 2016 and subsequent NDAAAs also implicitly acknowledge a degree of current vulnerability.

It is reasonable to assume that China and Russia share similar cyber vulnerability concerns and are pursuing assessments and remedial actions comparable to those in the United States, albeit without publicizing these efforts. As indicated, however, such defensive measures that may be adopted by any of these parties can never provide certainty that they have blocked all cyber intrusions. Thus, some degree of impairment of nuclear weapon systems, acknowledged or not, appears to be a chronic and ultimately irremediable potential threat for all three states.

**Cyber Operations Against Critical Infrastructure**

If the uncertainty and transparency generated by CNWS-cyber operations may have reduced the inclination of China, Russia, and the United States to resort to nuclear weapons in some settings, other developments are underscoring the growing utility of CCI-cyber strikes as a strategic tool. Such cyber assaults are not a substitute for nuclear assessments and remedial actions comparable to those in the United States, albeit without publicizing these efforts. As indicated, however, such defensive measures that may be adopted by any of these parties can never provide certainty that they have blocked all cyber intrusions. Thus, some degree of impairment of nuclear weapon systems, acknowledged or not, appears to be a chronic and ultimately irremediable potential threat for all three states.
Russia’s use of this tool against Ukraine’s electrical grid (noted earlier), North Korea’s interference with the international banking system, and Iran’s attempt to contaminate elements of Israel’s water supply display the potential of such intrusions. So do the 2021 ransomware attacks against the US petroleum product pipeline operator, Colonial Pipeline, and the important US meat processing firm, JBS USA. Separately, Washington has accused Moscow of readying CCI-cyberattacks against the US electrical power grid, reportedly leading the Trump administration to attempt to deploy its own cyber tools against Russian electrical grid systems as a deterrent.

As noted, employed on a massive scale, CCI-cyberwarfare can wreak havoc on the Chinese, Russian, and US homelands on a level that would be hard to match with conventional weapons and could inflict such harm far more rapidly, while avoiding the far greater destruction and high risk of retaliation in kind caused by a substantial nuclear strike. If critical infrastructure attacks were used by both sides in a confrontation, the prospect of escalation to the nuclear level would loom larger as the scale of infrastructure attacks intensified, but it is also possible that the cyber tool might cause sufficient pain to lead one or both parties to sue for peace, terminating hostilities and avoiding further escalation, including to the nuclear level.

It may be added that these three states are already engaged in a degree of cyberwarfare in the form of cyber espionage and data and intellectual property theft, with the United States, at least, known to have carried out retaliatory attacks against certain government-linked foreign agencies deemed to be behind attacks against US assets. Whatever dormant capabilities they may have clandestinely emplaced, however, all sides appear to have avoided directly launching widescale attacks against each other’s critical infrastructures. This restraint may be eroding, however. The ransomware attacks against Colonial Pipeline and JBS USA, as well as contemporaneous attacks against Western medical facilities, are all believed to have been perpetrated by entities associated with, or at least tolerated by, the Russian government, and represent significant departures from the norm of mutual restraint against damaging infrastructure attacks. These incidents serve as disturbing reminders of how lives would be placed at risk in a full-scale CCI-cyber assault and may have reinforced US concerns over possible Russian cyberattacks in response to Washington’s imposition of powerful financial sanctions against that country.

As these episodes exemplify, a cyber strike against critical infrastructure might have additional appeal because, although attribution capabilities have improved
in recent years, it would be considerably more difficult to attribute such a strike compared to one using conventional or nuclear weapons. Even when correctly attributed to a particular actor or organization, the link to a national government may be ambiguous. This could allow the country behind the cyberattack to seize an advantage during the period of disarray after the attack and before such time as the victimized state gained sufficient confidence to attribute the attack and mount a retaliatory strike. Attribution uncertainty might also temper the severity of any retaliatory action. The May 2021 Colonial Pipeline ransomware attack is a case in point. It remains uncertain whether the Russian hacking gang thought to have perpetrated the attack was acting independently, or with the support of or even at the direction of the Russian government. A further appeal of exploiting the CCI option is that critical infrastructure appears to be a highly vulnerable target.

Given the policies of Beijing, Moscow, and Washington to include CCI-cyber operations as a pre-nuclear escalatory option, the great flexibility of such cyber interventions, and their history of actual use, it is hard to imagine that such cyber operations will not come into play should a China-US crisis unfold in northeast Asia or a Russia-US confrontation erupt in Eastern Europe, such as one stemming from Russia’s invasion of Ukraine. Nuclear weapons will certainly form a backdrop to such encounters, their use restrained at least fractionally by concerns over cyber sabotage against these systems. In contrast, some level of counter-critical-infrastructure cyber aggression, tailored to the exigencies of the moment, is far more likely to actually be employed.

Exploring the New Strategic Paradigm

The above analysis has attempted to provide an overview of the strategic dimensions of Chinese-US and Russia-US cyber relations today, stemming specifically from two key offensive capabilities, but it has also identified many ambiguities and uncertainties. Thus the new paradigm of strategic affairs, with its cyber-tainted mutual uncertain destruction, high-impact CCI-cyber threats, and inherent opacity, remains amorphous and unsettled. This still-nascent condition, however, creates opportunities to influence the evolution of a common understanding of relevant governments regarding these issues—ideally a common understanding that supports strategic stability and, possibly, reduces the threat of nuclear conflict in some settings. Brief examinations of cyber impacts on bilateral nuclear deterrence, extended deterrence, bilateral nuclear arms control, and prospects for nuclear disarmament illustrate that common understandings in these areas are yet to be formed—and
that shaping such understandings to reduce nuclear risks will require serious effort.

**Bilateral Nuclear Deterrence**

As suggested earlier, in the cyber era, strategic stability based on the certainty of retaliation with nuclear arms no longer exists in its purest form. But the underlying premise behind this concept, also known as the nuclear revolution, is that certainty of retaliation meant that neither side of a nuclear dyad had an incentive to strike first. Although unqualified certainty of retaliation may no longer be at hand, it still remains true that neither side has an incentive to strike first because, as noted, the malware implanted by the country that is the intended target of a first strike would provide an additional source of early warning of an impending attack and put the successful execution of the first strike at risk, while the target country could reinforce its retaliatory response using any surviving nuclear assets by launching an accompanying massive CCI-attack. Early warning would be provided through multiple intelligence channels, now enhanced by a cyber channel operating within the would-be first-strike country’s nuclear weapon systems. How much early warning time might be provided is difficult to estimate, but it would seem to be a good deal longer than that which is required to activate the target country’s CNWS-malware to effectively interfere with the potential nuclear first strike.

What if the first-strike country combines its nuclear assault (of uncertain effectiveness) with a cyber assault on the target country’s nuclear weapon systems (also of uncertain effectiveness because of its untested malware), hoping to disable any target-country nuclear weapons that survive nuclear destruction? This may possibly give the first-strike country a greater chance of success, but even its combined attack remains a roll of the dice, risking annihilating retaliation. Indeed, certainty of retaliation is not necessary; a material probability of retaliation—game theorists would need to calculate the precise level—should do the job. In this scenario, although the threat of retaliation may no longer be as certain as in the past, it seems “sure enough.” In effect, a strong case can be made—and needs to be made—that the reliability of nuclear arms remains sufficient for deterrence, but not sufficient for preemption.31

Deterrence also operates to address cyber threats to critical infrastructure which, unlike CNWS-operations, are being openly discussed by governments and increasingly demonstrated by governments and third parties thought to be
closely linked to governments. Deterrence in this setting appears to be taking two forms: first, the threat of retaliation in kind, with CCI-strikes against the aggressor’s critical infrastructure, and second, the threat of retaliation escalated to using nuclear weapons.

There are many factors that would argue against escalation, not the least of which is that the target of the initial nuclear strike would be all too likely to retaliate with a nuclear riposte of its own. In addition, the state considering first-use of nuclear arms must also recognize that even a narrowly focused attack might fail because of hidden adversary malware. In that case, the adversary would also learn that its previously untested malware was effective, giving it the upper hand in any subsequent diplomatic or military engagement. In essence, to be the first to attempt to use nuclear arms in this particular setting—or indeed in any setting—is to risk disclosing a grave vulnerability that, prior to attempted use, remained uncertain.

Finally, it is worth reiterating the point made above that using CCI-cyberattacks may also reduce the risk of escalation to the nuclear level by providing additional, pre-nuclear rungs on the escalation ladder. At a lower level of destructiveness, such attacks may serve as powerful signals of resolve and at higher levels of destructiveness may prove so harmful as to lead to termination of hostilities before nuclear weapons are introduced.

**Extended Deterrence**

Of the three states under discussion, only the United States has given treaty-based pledges to defend other countries. Specifically, the United States has made commitments to its NATO allies as well as to Japan, South Korea, and Australia that it will defend them in any confrontation with a foreign enemy, even to the extent of using nuclear weapons on their behalf. This posture, known as “extended deterrence,” has always faced a question of credibility because of concerns on the part of US security partners that Washington would not stand by its obligations if this led to nuclear threats to the US homeland.

Beyond reinforcing allied defenses against external threats, extended deterrence also works as an important nonproliferation tool. US nuclear-backed security assurances, by offering an alternative mechanism for guaranteeing national security, provide a counter to pressures within NATO countries, and even more so in Japan and South Korea, for the development of independent nuclear arsenals. This further underscores the importance of sustaining the extended deterrence relationship.

The United States has worked assiduously and successfully for many years to reaffirm its defense commitments and dispel concerns about such political “decoupling,” in the case of NATO even to the extent of basing US nuclear
weapons in five NATO countries. The cyber threat to US nuclear forces inevitably makes the reassurance task more difficult, because now the United States must also persuasively reassure security partners that US nuclear weapons remain a reliable and effective deterrent against enemy aggression, notwithstanding the threat of cyber compromise. Since, as noted earlier, it may not be possible for the United States to determine the actual status of its nuclear arms given the presumed invisibility of adversary malware, this second “cyber” reassurance requirement would seem inherently difficult to satisfy.

Nonetheless, Washington appears to have met this challenge, as the June 14, 2021 Brussels NATO Summit communique makes clear. The document reiterates, with considerable emphasis, that nuclear deterrence remains intact, stating that “the Allies’ goal is to continue to bolster deterrence as a core element of our collective defence and ... in response to the more challenging security environment, NATO has taken steps to ensure its nuclear deterrent capabilities remain safe, secure, and effective.” Japan and South Korea have also reiterated their confidence in US nuclear-backed security assurances in similar joint declarations.

Quite possibly, if the cyber threat to US nuclear arms receives greater public attention in the future, US allies’ anxieties will grow. If so, it will be necessary to build the case noted in the previous section of this paper that, cyber challenges notwithstanding, nuclear deterrence still holds—albeit on terms different from those of the pre-cyber era.

**Bilateral Nuclear Arms Control**

Although rarely acknowledged by policymakers today, the concept that CNWS-cyber operations have eroded the reliability of nuclear arsenals is likely to become more widely accepted in coming years as an enduring condition. This development could pose difficulties for the future of some nuclear arms control measures by creating pressures to increase the diversity of nuclear weapon platforms and possibly the number of deployed weapons. Such pressures could arise on the theory that the larger and more multi-faceted a nuclear arsenal, the more likely at least some weapons would work as planned, notwithstanding adversary cyber sabotage efforts. Such concerns could well to lead to domestic political pressures in the United States to diversify and possibly enlarge US nuclear forces, the more so because of ongoing actions by Russia and China—the former diversifying its nuclear weapon systems within existing treaty limits, and the latter, not bound by treaty obligations, increasing both the size and

**The cyber threat makes reassurance and extended deterrence more difficult**
diversity of its nuclear deployments. Russia and China, continuing to be concerned about the impact of US cyber capabilities and missile defenses on their deterrents, may likewise have reason to be uncomfortable about participating in new arms control restrictions.

Anticipating these looming challenges, champions of classic nuclear arms control measures will need to build a case that the benefits of constraining open-ended nuclear arms racing through further reductions, or at least of extending current ceilings, outweigh any incremental increase in vulnerability to the cyber threat that such restrictions might engender. It might be argued, for example, that the cyber threat against nuclear forces has been part of the strategic environment for at least a decade and did not impede the negotiation and entry into force in 2011 of the New START Treaty. Nor did it apparently interfere with the treaty’s recent five-year extension, even as the cyber threat to nuclear weapon systems was gaining added attention in policy circles. In effect, as argued above, even in the face of the erosion of reliability, deterrence remains effective. In addition, there may also be strategies for diversifying nuclear platforms without increasing warhead numbers, such as keeping some legacy systems in use alongside modernized ones, thus multiplying the number of systems adversaries would need to impair to have a significant impact on national deterrents.36

Nuclear Disarmament

CNWS-cyber operations may open the door to additional approaches to nuclear disarmament beyond the classic focus on the gradual removal of such arms from national arsenals and their ultimate physical elimination. These alternatives, rather than focusing on the physical elimination of nuclear weapons, explore the possibility that such cyber operations could fatally impair nuclear arms, rendering them effectively unusable.

The discussion of mutually unassured or uncertain destruction in studies cited earlier by Danzig as well as by Miller and Fontaine, and in a scenario presented by Andrew Futter and Benjamin Zala, offer formulations of this possibility. Futter and Zala provide the most detailed elaboration of this concept (using the term “strategic non-nuclear weapons (SNNW)” to refer to CNWS-cyber operations): “It is also possible that this could be the pathway to a disarmed world and the end of the nuclear era, as SNNW cancel out any perceived advantages of nuclear weapons and increase the risks and trade-offs of relying upon them; disarmament through technological change rather than moral, political, economic, or diplomatic pressure. This scenario could see non-nuclear capabilities replacing nuclear weapons as the go-to technology for security and power, and states
relying on conventional and unconventional weapons for deterrence rather than nuclear: SNNW would provide general security.\textsuperscript{37}

All of these authors have carefully caveated their discussion of this possibility, but their initial thinking has opened an important and innovative dimension of discourse on these issues. This vision may seem exaggerated, but the cyber-induced strategic uncertainties on which it is based appear to be very real.

Creating the New Strategic Paradigm

The foregoing analysis suggests that despite the presence of CNWS- and CCI-cyber operations, it may be possible to sustain strategic stability, preserve US extended deterrence, create conditions for new arms control agreements, and make a degree of progress in reducing the salience of nuclear weapons and likelihood of their use. This, however, will depend on China, Russia, and the United States developing a common, if tacit, understanding on these issues, while deflecting pressures that would take events in less favorable directions. If cyber-era nuclear relations are to achieve a certain stability based on removing incentives to strike first, for example, Beijing, Moscow, and Washington must share a common appreciation that they are each vulnerable to adversary cyber operations directed at their nuclear forces, creating uncertainty that makes striking first with nuclear arms at least as fraught with danger and as unattractive as in the pre-cyber era.\textsuperscript{38} Similarly, these antagonists need to establish common understandings as to the escalatory potential of various CCI-cyberattacks and the likelihood of powerful retaliation in certain cases, an appreciation that could create a valuable element of mutual deterrence in this sphere of competition.

These various understandings could be achieved by unilateral declarations of policy, strategic dialogue with adversaries, and efforts to establish an international consensus on certain norms of cyber behavior, even if the last may be unenforceable as a practical matter.\textsuperscript{39} Secrecy or political considerations may restrict discussion of some sensitive issues; what state, after all, would wish to acknowledge potential flaws in the reliability of its nuclear arsenal? Academic and non-governmental policy specialists, however, through unclassified publications and professional meetings, could play an important role in promoting this potentially stabilizing conceptualization of emergent cyber-permeated nuclear relations—much as Thomas Schelling, Herman Kahn, Bernard Brodie, and other prominent analysts helped crystalize a stabilizing pre-cyber vision of
nuclear deterrence and arms control that gained broad international acceptance during the Cold War.

It is hard to argue that the advent of the offensive cyber operations discussed here has made the world a safer place. For better or worse, however, the trends described above appear to have become a part of the national security landscape and cannot be wished away. If the many dangers inherent in this new, largely opaque state of affairs can be managed, there may be benefits to be reaped from the caution that cyber uncertainties may instill in nuclear weapon operations and from the advent of added options for strategic competition short of nuclear war. Still, the associated risks of unpredictable escalation, unintended consequences, and miscalculation cannot be disregarded. Achieving any benefits from the emergent cyber-nuclear environment, while mitigating such cyber risks, will depend on the actions of strategic analysts and decisionmakers in the United States, China, and Russia. Hopefully, they will strive to shape the new strategic reality to enhance international stability and reduce the risk of nuclear conflict.

Notes


7. On the potential destructiveness of CCI-cyberattacks, see note 14.


19. See e.g., Borghard and Lonergan, “Cyber Operations as Imperfect Tools of Escalation.”

20. For an opposing view, see Futter and Zala, “Strategic Non-Nuclear Weapons.”


22. See Arbatov, “A New Era of Arms Control.”


31. See Miller and Fontaine, Navigating Strategic Pathways, 18.


36. This approach builds on a proposed strategy for strengthening cybersecurity of U.S. nuclear command, control, and communications suggested by Dr. Herbert Lin during a presentation at George Washington University’s Elliott School of International Affairs, May 18, 2021, https://blogs.gwu.edu/elliott-iistp/events-at-the-institute/nuclear-policy-talks/.

37. Futter and Zala, “The Third Nuclear Age,” 274.
