CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE

SHANGHAI INSTITUTES FOR INTERNATIONAL STUDIES

WORKING PAPER

APRIL 2021

China-U.S. Cyber-Nuclear C3 Stability

Ariel E. Levite, Lyu Jinghua, George Perkovich, Lu Chuanying, Xu Manshu, Li Bin, and Yang Fan

China-U.S. Cyber-Nuclear C3 Stability

Ariel E. Levite, Lyu Jinghua, George Perkovich,
Lu Chuanying, Xu Manshu, Li Bin, and Yang Fan

We wish to thank the Carnegie Corporation of New York for its generous grant that enabled us to conduct this project and publish this paper.

Carnegie Endowment for International Peace
Publications Department
1779 Massachusetts Avenue NW
Washington, DC 20036
P: + 1 202 483 7600
F: + 1 202 483 1840
CarnegieEndowment.org

This publication can be downloaded at no cost at CarnegieEndowment.org.

CONTENTS

About the Project

This paper was produced through a dialogue between a Carnegie expert team in consultation with several external experts and a corresponding Chinese team.

The Carnegie team consisted of George Perkovich, Ariel E. Levite, Lyu Jinghua, Katherine Charlet, Michael D. Swaine, and Wyatt Hoffman. The U.S. experts consulted included Robert Schmidle and John A. Davis. (Please note that the list of Carnegie experts includes some individuals that have since departed Carnegie.)

The Chinese team was comprised of Lu Chuanying, Xu Manshu, Li Bin, and Yang Fan. The Chinese experts consulted included Xu Weidi, Lu Yin, Zhao Wuwen, Kang Chunmei, Hui Zhibin, Dai Lina, Shen Yi, Cai Cuihong, Lang Ping, Zhang Tengjun, Tong Zhao, Wu Chunsi, Ye Jiang, and Feng Shuai.

The authors also wish to thank the other institutions and individuals who contributed to the paper but do not appear on the list of acknowledgments above.

About the Carnegie Endowment for International Peace

The Carnegie Endowment for International Peace is a unique global network of policy research centers in Russia, China, Europe, the Middle East, India, and the United States. Our mission, dating back more than a century, is to advance peace through analysis and development of fresh policy ideas and direct engagement and collaboration with decisionmakers in government, business, and civil society. Working together, our centers bring the inestimable benefit of multiple national viewpoints to bilateral, regional, and global issues.

About the Research Center for Global Cyberspace Governance

The Research Center for Global Cyberspace Governance, the Shanghai Institutes for International Studies (SIIS), is a think tank specialized on the topics of cybersecurity and global cyberspace governance, with the purpose of exploring the global cybersecurity landscape and national cybersecurity strategies, while promoting the creation of global cyberspace governance mechanisms. The Research Center for Global Cyberspace Governance was founded in December 2018 in a joint effort by the Shanghai Institutes for International Studies, the PLA National Defense University, Fudan University, Nanjing University, Xiamen University, the Shanghai Academy of Social Sciences, and others.

The center serves the highest levels of Chinese policymaking in the areas of cyberspace administration and foreign relations, among others. To this day, the center has developed cooperation with various organizations, including the UNICRI Centre for Artificial Intelligence and Robotics, the UN Commission on Crime Prevention and Criminal Justice, the Massachusetts Institute of Technology, the Carnegie Endowment for International Peace, the Center for Strategic and International Studies, the Russian Academy of Military Sciences, the University of Leiden in Netherlands, and others.

About the Participants

Ariel (Eli) Levite is a nonresident senior fellow in the Nuclear Policy Program and Cyber Policy Initiative at the Carnegie Endowment.

Cai Cuihong is a professor at Fudan University.

Dai Lina is an associate research fellow in the Center for Internet Studies at the Shanghai Academy of Social Sciences.

Feng Shuai is an associate research fellow at SIIS.

George Perkovich is the Ken Olivier and Angela Nomellini Chair and vice president for studies at the Carnegie Endowment, overseeing the Technology and International Affairs Program and Nuclear Policy Program.

Hui Zhibin is a senior research fellow in the Center for Internet Studies at the Shanghai Academy of Social Sciences.

John A. Davis, a retired major general, is the vice president and federal chief security officer for Palo Alto Networks and former deputy assistant secretary of defense for cyber policy.

Kang Chunmei is a senior research fellow in the China Academy of Engineering Physics.

Katherine Charlet is the director for data governance, government affairs, and public policy at Google and former director of the Technology and International Affairs Program at the Carnegie Endowment.

Lang Ping is a senior research fellow in the Institute of World Economics and Politics at the Chinese Academy of Social Sciences.

Li Bin is a professor in the Department of International Relations at Tsinghua University and a former senior fellow in the Nuclear Policy Program and Asia Program at the Carnegie Endowment.

Lu Chuanying is the director of and a senior fellow at the Research Center for Global Cyberspace Governance, SIIS.

Lu Yin is an associate professor at the School of National Security at the National Defense University of the People's Liberation Army of China.

Lyu Jinghua is a visiting scholar in the Cyber Policy Initiative at the Carnegie Endowment.

Michael D. Swaine is the director of the East Asia Program at the Quincy Institute for Responsible Statecraft and former senior fellow in the Asia Program at the Carnegie Endowment.

Robert Schmidle, a retired lieutenant general, is the university adviser on cyber capabilities and conflict studies at Arizona State University, a professor of practice in the School of Politics and Global Studies, a senior fellow in the Center on the Future of War, and former deputy commander of the U.S. Cyber Command.

Shen Yi is a professor at Fudan University.
Tong Zhao is a senior research fellow in the Nuclear Policy Program at the Carnegie–Tsinghua Center for Global Policy.

Wu Chunsi is the director of the Institute for International Strategic Studies at SIIS.

Wyatt Hoffman is a research fellow at the Center for Security and Emerging Technology and former senior research analyst with the Nuclear Policy Program and the Cyber Policy Initiative at the Carnegie Endowment.

Xu Manshu is a senior fellow at the Research Center for Global Cyberspace Governance at SIIS.

Xu Weidi is a former senior fellow at the Institute for Strategic Studies, National Defense University of the People's Liberation Army of China.

Yang Fan is the deputy director of the Cyberspace International Law Center at the Xiamen University School of Law.

Ye Jiang is a senior research fellow in the Institute for Global Governance Studies at SIIS.

Zhao Wuwen is a senior research fellow in the China Academy of Engineering Physics.

Zhu Lixin is a professor in the Cybersecurity Law Institute at the Xi'an Jiaotong University.

Forewords

Chen Dongxiao

The impact of cyber on nuclear stability is one of the most forward-looking and strategic topics in the current international security field. The Shanghai Institutes for International Studies (SIIS) and Carnegie Endowment for International Peace (CEIP) have conducted a joint study around this topic, aiming to provide a reference for the establishment of cyber and nuclear stability mechanisms among nuclear states.

Cyber attacks on nuclear command, control, and communications (NC3) systems have become a potential source of conflict escalation among nuclear powers. Yet major powers have not established effective risk-reduction mechanisms in this regard. While information technology strengthens nuclear strategic forces in many ways, including the modernization of NC3, it also poses an increasingly serious cyber threat to nuclear command and control systems. Cyber operations against the strategic command and control systems of nuclear states—including those probing major vulnerabilities in the command and control systems and satellite communications systems, cyber threats from third parties, and the lack of strategic trust in cyberspace—have exacerbated the impact of cybersecurity on nuclear stability.

Because of the unique nature of nuclear weapons, any cyber incidents concerning nuclear weapons would cause state alarm, anxiety, confusion, and erode state confidence in the reliability and integrity of nuclear deterrent. Cyber attacks against a nuclear command and control system would expose the attacked state to significant pressure to escalate conflict and even use nuclear weapons before its nuclear capabilities are compromised. At the same time, compared to the mature experience and full-fledged mechanisms in nuclear deterrence, crisis management, and conflict escalation/de-escalation among the traditional nuclear powers, states not only lack a comprehensive and accurate perception of the threat posed by cyber operations but also lack consensus on crisis management and conflict de-escalation initiatives.

Given that not enough attention has been paid to this new type of threat on the agenda of security dialogue between nuclear powers, SIIS and CEIP launched a joint research project on cyber and nuclear stability in U.S.-China relations in 2017, focusing on exploring the possibility of building consensus and agreement among nuclear states. It is hoped that the cyber-nuclear nexus will awaken national policymakers to the urgency of maintaining cyber stability and that nuclear states will fully recognize the dangers of cyber attacks and their respective vulnerabilities to such attacks, and thus take steps to reduce nuclear instability accompanying advancing cyber technologies and prevent nuclear war.

China and the United States are cyber powers with nuclear strategic capabilities. While the United States and China have differences of interests and priorities in cyberspace, there is still common interest in dialogue and cooperation for stability. I note that before taking office, U.S. President Joe Biden asked five questions about science and technology policy, including one on how the United States can "ensure the long-term health of U.S. science and technology."[1] China's President Xi Jinping has repeatedly stressed the need to "ensure that the more than 1.3 billion Chinese people and people across the world can all enjoy the benefits of Internet development."[2] Obviously, with today's evolving information technology, it is in the interest of both countries to avoid war and reduce conflicts that may escalate into war, and it is both the international responsibility of major powers and the common expectation of the international community. Hopefully, this joint study will promote in-depth dialogue and security cooperation between China and the United States and establish a corresponding workable and professional mechanism.

This joint study is a rigorous academic research project, a joint achievement of the Chinese and American research teams. The two teams have worked together for four years, with international seminars (in Shanghai on January 13, 2018, and in Beijing on March 25, 2019), working group meetings (in Washington on March 20, 2017, and in Beijing on June 4, 2017, October 24, 2018, and November 5, 2019, respectively), and more than ten online seminars. During this period, experts in relevant fields and government departments were closely consulted. Based on the final draft in English, teams from both sides translated, revised, and proofread word by word to form the final joint publication in English and Chinese.

This is an important joint study released by two prominent think tanks in China and the United States, hoping to improve mutual understanding between China and the United States on each other's security concerns, interests and solutions to problems, promote stability in China-U.S. relations, and facilitate the healthy development of overall China-U.S. relations. I also believe it has important reference value for the two governments on how to bridge differences and forge consensus in sensitive areas. I would like to congratulate the research teams on their achievement and, in particular, thank the CEIP research team for their tireless efforts to travel between the United States and China many times and work closely with the Chinese research team. I also hope that SIIS and Carnegie will continue to conduct joint research around U.S.-China cybersecurity issues and make greater contributions to U.S.-China relations. As always, SIIS is grateful for financial support from the China-United States Exchange Foundation (CUSEF) to help SIIS taskforces conduct joint research on U.S.-China relations, including this pathbreaking work with CEIP.

Chen Dongxiao, President of the Shanghai Institutes for International Studies

Thomas Carothers

Military and national security experts increasingly warn that the most likely cause of major warfare—conventional or nuclear—between the United States and China is a minor conflict that escalates sharply, even despite the desires and efforts by one or both countries to avert such a spiraling disaster. Cyber operations, whether by China against the United States, or vice versa, are especially prone to provoking an escalation. It is very difficult for officials who detect an intruder in their country's strategic computer networks to determine the intruder's intentions. These intentions might be primarily defensive—seeking to gain warning of a future attack. But they might be offensive—precursors of efforts to disrupt or destroy the functioning of warning systems and/or command and control and communications systems related to a nuclear deterrent. Without knowing what an intruder is seeking to do, those who detect the digital footprints of an intrusion may well assume the worst. Pressure could thus mount quickly to strike first, before the other side can make this more difficult or even impossible.

Such risks are especially evident between the United States and China because these two powers, unlike the United States and Russia, have never defined their strategic relationship as one of mutual vulnerability, with attendant understandings of how to stabilize it. The asymmetry between their nuclear forces and other offensive and defensive capabilities may incline Chinese officials to assume that the United States will at some point act on the temptation to negate China's nuclear deterrent. Chinese actions, especially in the cyber domain, to try to avoid such a possibility might make U.S. officials fear that China is seeking to impede the U.S. nuclear deterrent.

These risks will grow as dual-use systems—satellites, missiles, or command and control systems that are used both for potential conventional and nuclear warfare—are deployed by one side or the other. An adversary may intend only to preempt or retaliate against conventional war-fighting capabilities, but the target of the attack could perceive them to be directed against or at least affecting its own nuclear forces.

This pathbreaking paper, which is being published in English and Mandarin, calls attention to these rising dangers. It is the product of a unique multi-year joint venture between the Shanghai Institute for International Studies and the Carnegie Endowment for International Peace. It aims to provide a robust open-source foundation for discussion of these issues in both China and the United States, overcoming the barriers of high classification and institutional compartmentation that frequently

impede analysis and deliberation. The co-authorship of the paper by Chinese and U.S. teams also aims to overcome (at least partially) barriers of culture and language that render mutual understanding in this domain so difficult.

The paper begins by detailing plausible scenarios of grave concern and providing a framework for analyzing them. It then explores steps that the U.S. and Chinese governments—and, with their encouragement, nongovernmental groups such as think tanks in both countries—could take to diminish inadvertent cyber threats to nuclear command, control, and communication systems. These are steps that could be undertaken unilaterally or bilaterally, through reciprocity or negotiation. The report also offers topics for dialogue that relevant officials—whether diplomats, military officers, cyber operators, computer emergency response teams, or others—could pursue to help stabilize relations and sketches an agenda for confidence-building that they might pursue.

Both groups of authors consulted with former and current experts from their governments to ensure a close grounding in current policy and technological realities. Although official relations between the two governments deteriorated significantly during the span of the project, the two teams of authors and the host organizations remained constructively focused on the critical objectives of enhancing mutual understanding of the risks that both countries face at the cyber-nuclear nexus and finding a cooperative path for reducing risks. At the personal and institutional levels, they found it simple to remain cooperative given the stakes involved, a dynamic that has become unfortunately elusive in the overheated discourse of strategic rivalry within and between both countries.

The Carnegie Endowment is grateful to the Carnegie Corporation of New York for financial support that helped make this paper possible, and for many years of partnership in working to help reduce the global risks of nuclear conflict.

Thomas Carothers, Interim President of the Carnegie Endowment for International Peace

Summary

Cyber threats to nuclear command, control, and communications systems (NC3) attract increasing concerns.[3] Prominent experts in the West have published reports and articles analyzing the full scale of risks. They conclude that cyber operations could threaten—intentionally or unintentionally—the functions of nuclear systems and thus unleash highly adverse strategic dynamics. These dynamics could turn crises into armed conflicts and armed conflicts into nuclear war. Chinese scholars and officials do not explicitly discuss these concerns, but they use past examples like Stuxnet to flag ways that cyber attacks could undermine nuclear stability.

Recognizing the shared interest in diminishing the prospects of accidents, inadvertent conflict, and escalation, the Carnegie Endowment for International Peace convened experts from the United States and China to discuss generic cyber-nuclear challenges, analyze pertinent scenarios of cyber threats to NC3, and recommend possible steps that both countries could take unilaterally or collaboratively to ameliorate them. Drawing on public sources of information, we have developed a common base of pertinent unclassified knowledge in both English and Chinese that could serve as a platform for more discreet engagements between the respective authorities of both countries.

This paper begins by briefly setting the context in which concerns arise about cyber operations against NC3. As China-U.S. relations evolve toward intense great-power competition, the classical security dilemma has intensified in recent years. Each side questions the other's conception of strategic stability and doubts their intention to maintain it, however stability is defined. Neither sees the other restraining itself from competitive, if not aggressive, actions. There is no apparent effort to build mutual trust.

The United States worries especially that China will not eschew the use of force in territorial disputes with its neighbors, several of whom are U.S. allies or partners. American strategists worry that China is increasing its cyber, conventional, and nuclear capabilities in order to undermine the United States' extended deterrence guarantees and prevent it from defending its allies. China's principal concern, on the other hand, stems from perceptions that the United States seeks superior cyber, conventional, and nuclear capabilities that could be used to conduct first strikes against China's nuclear deterrent and blunt its retaliatory capability.

These conflicting threat perceptions, together with the significant disparity in the two countries' nuclear arsenals, make it extremely difficult to produce and negotiate a common approach toward strategic stability that each side can trust and verify.

Although the United States and China had until recently maintained a dialogue and engaged in some cooperation, friction in the cyber domain has become incessant and increasingly intense. Capabilities to conduct cyber operations for espionage, covert operations, and attack are alluring for many reasons. They are relatively inexpensive, nonlethal, often effective, and not clearly illegal. Because they seem—and often are—less destructive, more temporary in their effects, and generally less provocative than the use of human spies and certainly kinetic weapons, cyber operations pose a lower risk of escalation. Their secrecy may also diminish the associated risks: because the targeted party's public will not know about the attack, leaders don't face public pressure to respond. Thus, both China and the United States have increased their cyber capabilities and elevated the role these capabilities play in their overall security postures. And, because both sides place so much value on their nuclear deterrent, each is deeply alarmed by the possibility that the other would be tempted to threaten it with cyber weapons.

Despite their shared interest in understanding and mitigating cyber-nuclear risks, two fundamental factors have impeded American and Chinese policymakers. First, deep distrust pervades the bilateral relationship—neither side is confident that their reassurances would actually bolster stability. Second, the two sides differ on what must be done to begin making progress. The United States insists that little can be done if China will neither publicly acknowledge possession of offensive cyber capabilities nor profess a willingness to discuss their use. China, on the other hand, wants the United States to acknowledge that Washington has superior cyber capabilities and that its cyber strategy could threaten China's second-strike deterrent. Finally, there is a thorny political-psychological factor: Chinese officials believe that trust must be built before concrete conflictual issues can be resolved; U.S. officials believe, conversely, that concrete actions (often involving self-restraint) constitute the primary way to build trust.

Against this background, this paper describes types of cyber operations that states could be tempted to direct against an adversary's NC3 system. Espionage comes first. The temptation is strong—and this challenge severe—because intelligence gathered by penetrating NC3 systems would be highly valuable. Early-warning intelligence, which could inform whether and when an adversary is preparing to conduct nuclear strikes, is especially desirable. And such intelligence—or the belief that an adversary can acquire it—can then strengthen deterrence. The complexity, secrecy, and compartmentation of NC3 architecture further exacerbate the challenges. Cyber intrusions can enable cyber attacks even if the conductor is only intending to spy. The commonality and dual-use potential inherent in cyber operations obscure the aggressor's motivations, making it difficult for either side to predict the implications or potential consequences of any operation. The possibility that third-party actors—including other states, terrorists, or political subversives—may seek to use cyber operations

to foment China-U.S. conflict adds complexity to the situation. China or the United States could also disguise themselves as a third party when attacking the other (known as a false-flag operation), or activate proxies to conduct cyber operations against the other.

Three additional factors may exacerbate the potential for instability and conflict escalation in the China-U.S. context: the structure and doctrine of the two countries' command and control systems differ significantly. The two governments diverge in their perceptions of the balance of cyber capabilities between them. And China and the United States are developing and deploying cyber and conventional forces and command and control systems whose potential uses could increasingly become entangled with nuclear operations. Such entanglement could be purposeful or inadvertent but, either way, carries significant potential for destabilization.

Instead of describing all the ways cyber operations could go wrong, this paper identifies categories of scenarios that highlight the most destabilizing factors and the most worrisome risks to strategic stability. Four types of scenarios deserve especially intense consideration:

1. cyber espionage collecting data on and inside the core of an adversary's NC3 system;

2. cyber espionage occurring in dual-use systems or other elements that also support or are connected with NC3;

3. cyber attacks directed at dual-use (conventional alongside strategic) NC3 systems or auxiliary systems supporting or connected with NC3, without any intention to affect their nuclear functionality; and

4. circumstances that combine serious suspicions about the intentions of the other party with apprehensions about the vulnerability of one's own NC3 to adversary cyber attacks.

These scenarios suggest four broad types of strategically worrisome consequences: 1) nuclear conflict; 2) inadvertent or accidental use of a nuclear weapon; 3) crisis escalation; or 4) long-term destabilizing impacts such as arms racing and ensuing crisis instability. These risks are caused in part by how difficult it is for either party to predict the effects of cyber operations in advance or assess them afterward. The risks are exacerbated by the potential that third-party actors could sow confusion and exacerbate crises, the challenges of attribution, and the implications of two adversaries with asymmetrical attribution capabilities.

To date, both China and the United States share the desire to avoid inadvertently sliding into armed conflict and are committed to averting escalation toward nuclear war. Hence, it is meaningful and feasible to discuss possible measures they could take unilaterally and/or collaboratively to diminish inadvertent cyber threats to NC3. This is true despite secrecy constraints, the profound distrust of each other's intentions, divergent approaches to security challenges, and structural asymmetries in the two sides' capabilities and ways of thinking and acting in the cyber and nuclear domains.

Assured Decisionmaking Procedures for Cyber Operations

To reduce risks of ill-conceived cyber operations, the two sides should subject all such operations to robust oversight and risk management protocols. Mutual understanding of each side's approach to oversight also could help avoid exaggerating the threats they pose to each other. Assessment and control procedures should operate at five levels:

1. domestic and foreign policy oversight by competent national authority;

2. technical oversight to assess the intended effects and potential unintended consequences of cyber operations;

3. operational oversight to verify positive control within an authorized chain of command;

4. intelligence oversight to assess the consequences of exposure and potential loss of intelligence sources and methods, as well as how the insights will be affected if the cyber operation or capability is discovered or revealed; and

5. legal oversight to assess both the capability and the operation as it applies to applicable domestic and international laws and agreements.

All of this could be done unilaterally and in secrecy. But bilateral dialogue on these issues could produce additional benefits and help build mutual confidence.

Creating a More Stable and Less Vulnerable Strategic Context

The United States and China are naturally taking steps to modernize their nuclear architectures and forces, including their NC3 systems. To avoid the worst effects of security dilemmas—or worst-case assessments—the two governments could adopt mitigating measures. They could recognize and communicate with each other that some types of response to perceived threats are prudent and can be stabilizing. Both sides may want to increase the number, diversity, and modes of deployment of

nuclear systems over concerns about cyber attacks on their NC3. Both could also clarify their intentions and doctrines to help reduce the instabilities and risks of nuclear use and escalation, as they seek to lower restraints on readiness and nuclear use. Both sides can also work together to acknowledge that the development and deployment of new capabilities—such as anti-satellite weapons, space warfare, and artificial intelligence—will arouse concern about cyber-nuclear threats that deserve more attention.

Mutual Commitments on Restraints

As neither side sees a lasting advantage in entering large-scale armed conflict or employing nuclear weapons to avoid losing, this paper intends to explore some measures to restrain cyber capabilities and/or actions that threaten each other's NC3.

The first is the possibility of formally committing not to conduct any cyber intrusion into core NC3 systems. For heuristic purposes, this could take several forms: 1) both sides could agree on a generic description of core NC3 components; 2) each side could elect to designate some elements of its core NC3 systems and share the list with the other; or 3) without sharing with each other precisely what constitutes core NC3, each side could notify the other when it detects cyber intrusion from the other into some NC3 system elements that it believes play a core role, with the expectation that the intruder would then cease and withdraw immediately.

Chinese participants generally welcome such measures of self-restraint, but American experts largely find them either inadvisable or impractical. However, this does not entirely negate the value of internally analyzing the desirability and feasibility of such approaches and facilitating bilateral discussion of them.

A second form of restraint could be committing to subject cyber operations targeting NC3 to authorization by senior leadership in each country.

A third restraint worth exploring is whether the two governments could agree not to target space-based strategic assets of particular importance for NC3.

Fourth, both countries could address concerns over third-party cyber intervention in NC3 systems by committing to exercise effective oversight and control over actors that are: 1) under their direction; 2) using their territory to conduct operations; 3) employing capabilities developed by them; or 4) allies over whom they wield considerable influence. U.S. experts emphasize the shared interest in such steps while Chinese experts have doubted their feasibility in the current political environment. Nevertheless, we believe this form of restraint merits further consideration and dialogue.

Dialogue and Information Sharing

This entire paper and the preceding summary remarks point to the importance of sustained dialogue and information sharing. Whereas sustained dialogue has enabled the United States and Russia to create shared understanding of strategic stability and crisis management, no such foundation exists between the United States and China. This is especially disconcerting to China (and, therefore, more broadly) because mutual nuclear vulnerability has not been acknowledged as a basic condition of the relationship. The absence of this foundation makes it exceedingly difficult to redress each other's concerns over nuclear postures and cyber threats. Indeed, the two countries' conflicting views on whether and how to discuss military dimensions of cyber competition compound the challenge of conducting dialogue on cyber threats to strategic stability.

This paper identifies three main topics that would be essential to address in appropriate official settings. The first is to develop mutual understanding of the steps that one or both states find destabilizing and those that both agree are stabilizing. These would include capabilities, decisionmaking procedures, operations involving cyber instruments, and operations involving nuclear forces and NC3. A second topic would be the potential benefits and risks of offensive cyber operations, especially as they pertain to the cyber-nuclear nexus. Recognizing the extreme sensitivity and classification of these issues, such dialogue would necessarily operate at a general/generic level. Third, China and the United States could explore whether and how to share information on these issues during peacetime.

The subjects covered in this paper could be explored in new bilateral forums but could also tap existing ones. Among existing forums, the following could be utilized:

- the Diplomatic and Security Dialogue for high-level officials to express concerns over policy changes and share major developments;
- two Memoranda of Understanding (MOUs) for both militaries to discuss basic principles of conduct for cyber operations;
- the U.S.-China Joint Staff Dialogue for mid-level officials to discuss capabilities and intentions of cyber forces and concerns about perceived cyber threats to NC3 systems;
- the established channels between designated higher-level officials for communication during major cyber incidents or crises;

- the existing coordination mechanism between both countries' computer emergency response teams (CERTs) for continued cooperation and possibly broader information on threats with potential strategic consequences; and

- the existing hotline between the Chinese Ministry of National Defense and the U.S. Department of Defense for communication on cyber issues pertaining to NC3.

Ultimately, the threats that cyber operations could pose to NC3 and strategic stability are important enough that designing or choosing modalities for understanding and addressing them is a minor challenge. The real challenge is to generate the will to overcome the doubts, suspicions, and political fear that keep leaders of both countries from taking the initial steps necessary to convince each other that constructive moves will be reciprocated. This paper seeks to encourage such moves by laying down an unclassified agenda for discussion, clarifying the stakes involved, and suggesting possible steps the two countries could take to reverse dangerous trends—especially those that increase the risk of unintendedly escalating crises or conflict.

Introduction

Prominent experts around the world worry that cyber operations could threaten—intentionally or unintentionally—the functions of nuclear command, control, and communications systems (NC3). This could unleash highly adverse strategic dynamics, including even increased risks that crises could escalate to armed conflict and that armed conflict could escalate to nuclear war.[4] In crises or conventional military conflicts between nuclear-armed states, the presence—or suspected presence—of external cyber intrusions anywhere in their NC3 systems could cause human reactions and technical malfunctions that may be escalatory or otherwise highly destabilizing. This could happen even if the leaders of the states involved did not intend to escalate. Such dynamics could be caused by one or both conflicting states—or by third parties, including nonstate actors.

Existing Literature on Cyber-Nuclear Risks

Attention to cyber threats to nuclear systems has been growing for years. A 2009 study commissioned by the International Commission on Nuclear Non-proliferation and Disarmament argues that "cyber terrorists" could theoretically trigger a nuclear exchange or launch a weapon via cyber intrusion.[5] A 2013 report by the U.S. Department of Defense's Defense Science Board warned that most nuclear systems had not undergone end-to-end assessments for resilience against top-tier cyber threats.[6] While there has been little official acknowledgment, former military and defense officials continuously voice concerns over cyber threats publicly. For example, a former commander of U.S. Strategic Command, Gen. (ret.) James Cartwright, argued in 2015 that NC3 systems were vulnerable to cyber intrusion, and that the consequences could include nuclear use in response to a false warning of attack.[7] Former UK secretary of state for defense Des Browne charged the British government to conduct an end-to-end cybersecurity assessment of the UK's Trident systems to ensure cyber attacks couldn't disable the UK deterrent.[8] There is strong evidence that Russian military and defense officials are similarly concerned about cyber attacks aimed at disabling Russian command and control.[9] In February 2019, current and former senior officials from the United States, Europe, and Russia, along with several prominent institutions, called for dialogue to address cyber threats to NC3.[10] According to the legislation proposed by the House Armed Services Committee in June 2019, the U.S. Congress would boost funding for NC3, calling on the Pentagon to develop "near- and long-term plans and options to ensure resilience" of the NC3 network.[11]

A handful of studies have analyzed in depth the full scope of cyber-nuclear risks. Reports by Chatham House and the Nuclear Threat Initiative describe a range of scenarios including false detection of a nuclear attack, disruption of communications in a crisis, supply chain threats compromising nuclear systems, and cyber intrusions leading to unauthorized use of nuclear weapons.[12] In *Hacking the Bomb: Cyber Threats and Nuclear Weapons*, Andrew Futter describes how cyber threats might undermine mutually assured destruction and lead to a "gradual descent into a new era of 'aggravated' nuclear instability," generating anxieties and pressure to use nuclear weapons more rapidly.[13] In their report titled "Cyber War and Nuclear Peace," David C. Gompert and Martin Libicki (two prominent cyber scholars affiliated with leading U.S. defense think tanks) explore the nexus between revolutionary digital technologies and discuss the concerns that offensive cyber operations against the NC3 system of a major nuclear state might lead to a hair-trigger launch policy and even to nuclear war.[14] Jon R. Lindsay, in "Cyber Operations and Nuclear Weapons," focuses on the potential for offensive cyber operations targeting NC3 to cause organizational breakdown, decisionmaking confusion, and miscalculation in a nuclear crisis."[15] Other academic studies have described potentially destabilizing cyber-nuclear interactions in crisis or conflict resulting from the ambiguities and uncertainties of cyber operations.[16] Looking ahead, some warn that the introduction of artificial intelligence and machine learning capabilities into NC3 systems will exacerbate many of these risks.[17] While there is no official public discussion of these concerns, some Chinese scholars have considered the dynamics between cyber attacks and nuclear stability, mostly by analyzing past examples like Stuxnet.[18]

Two themes cut across all the concerns expressed about cyber and NC3 issues.

First, a number of factors make it practically impossible to fully understand and predict the cyber vulnerability of NC3 systems. These systems are inherently complex and are becoming more so every year. They typically include a mixture of old (legacy) components and modern elements. NC3 systems have been repeatedly modified, upgraded, and integrated piecemeal over many years to accommodate evolving requirements, technological changes, patching of vulnerabilities, and modernization. This makes it inherently difficult even for the relatively few individuals with sufficient security clearances to fully comprehend their structure and composition, let alone to identify their vulnerabilities. Moreover, these systems depend on, or are connected in various ways to, other systems that are dual- or multifunctional and not equally secure. All these links are challenging to map and fully assess. As nuclear states gradually integrate new technologies, especially artificial

intelligence, to enhance their early-warning, reconnaissance, and command and controls systems, they inevitably complicate them further. This could make these systems less comprehensible to their own operators as well as their adversaries.

Second, any information about NC3 and about offensive cyber operations and capabilities is subject to both exceptional secrecy and tight compartmentation. The people responsible for these various functions typically operate in separate, siloed communities with at most intermittent and superficial communication—let alone coordination—between them. As a result, officials responsible for NC3 and for cyber operations lack full appreciation of the risks that both functions may face or create. Senior decisionmakers at all levels may be entirely unaware, being inadequately informed about this tension and certainly not cognizant of the implications that flow from these dynamics. This, in turn, also impairs states' communications with each other, whether in declaring policies in peacetime or signaling intentions during escalating crises or conflict.

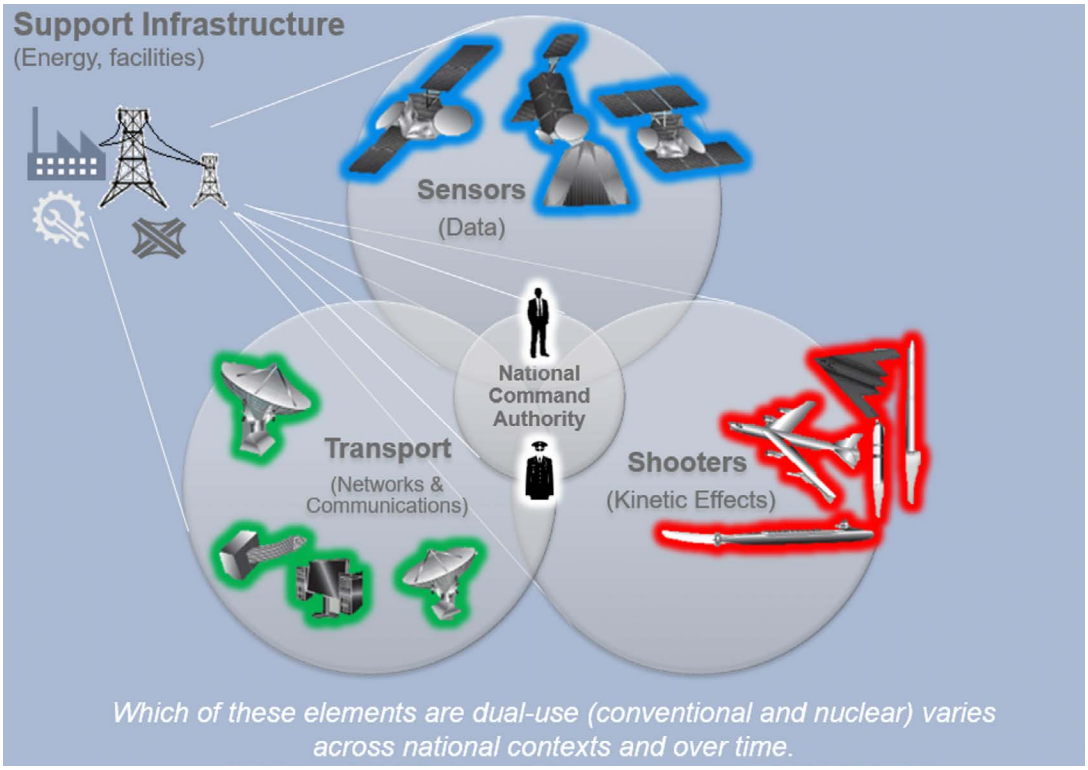
Another common concern, and one not fully covered by any of the reports listed above, is that third parties can increase the complexity of the situation. It is always difficult to attribute a cyber attack to its source with confidence, let alone in real time. Cyber-savvy nation-states can disguise themselves as other actors and initiate cyber attacks on others. This suggests the potential to do the same in NC3 systems as well. Russian actors reportedly penetrated Iranian hackers' systems and hijacked their hacking tools to compromise entities in at least thirty-five countries. Some victims of the hacks and security analysts may have initially thought the hacks were conducted by Iran, before it became evident that Russians were responsible.[19] In a separate cyber attack targeting the 2018 Winter Olympics, attackers reportedly planted sophisticated "digital fingerprints" in their malware, such as forged metadata mimicking North Korean malware, apparently designed to lead investigators to misattribute the attack. This attack, too, was ultimately traced back to Russian actors.[20] In addition to state actors, terrorists and other nonstate actors could create crises by pretending to be a state.

Recognizing the shared interest in diminishing the prospects of accidents, inadvertent conflict, and escalation, the Carnegie Endowment for International Peace convened experts from the United States and China to discuss generic cyber-nuclear challenges, analyze pertinent scenarios of cyber threats to NC3 systems, and recommend possible steps that both countries could take to ameliorate them—unilaterally or collaboratively. Participants based this work on public sources of information. Important details about cyber capabilities and NC3 systems are, of course, highly classified, and should remain so. Nevertheless, publicly available information gave the experts a sufficient basis to analyze and raise awareness of challenges as well as to explore possible means to manage them.

Based on public sources, we define nuclear command, control, and communications, or NC3, as the entire apparatus of information and telecommunications facilitating and supporting the operations of nuclear forces and assisting nuclear-weapons decisionmaking. Importantly, NC3 also includes auxiliary systems (such as power supplies) that are vital to their functioning and potentially vulnerable to cyber attack. Nuclear-armed states require NC3 to function from early warning all the way to conducting nuclear operations. For illustrative purposes, we include here a sketch of the components such a system entails.

FIGURE 1

Support Infrastructure for NC3 Systems



SOURCE: Modified from the "Nuclear Matters Handbook 2016," U.S. Department of Defense.

This paper begins by briefly contextualizing China-U.S. relations and the specific cyber dimensions of this relationship. Next, it summarizes a range of generic cyber threats that the participants have identified as possibly applicable to NC3. It then describes several scenarios of threats that partici-

pants deemed most worthy to address more fully in a Chinese-U.S. context. After exploring these scenarios, the paper lays out possible measures the United States and China could take unilaterally and/or collaboratively to reduce risks associated with such threats. Its intention is to invite experts and officials from the two countries—as well as the broader international community—to advance understanding of these issues and reflect on constructive ways to address them. Of course, responsibility for implementing any and all of the measures discussed in the concluding section of this paper resides exclusively with the competent authorities in the United States and China, or any given nuclear-armed state.

Strategic Stability: The Importance of Context

Before discussing the specific cyber-nuclear nexus, it is helpful to consider the strategic and domestic contexts in which concerns about cyber operations against NC3 arise. Context often shapes the approach actors take toward any concrete issue and defines the options available to address concerns. For our purposes here, the broader context is the nature of strategic relations between the parties, their broad conception of security in general, and nuclear posture in particular.

A major challenge in defining strategic stability between the United States and China is that the two states—unlike the United States and Russia—lack a common definition of strategic stability and have differing concerns. The United States does not base its policies toward China on the principle of mutual vulnerability, as it does with Russia.[21] Accordingly, China's principal concern stems from perceptions that the United States seeks superior cyber, conventional, and nuclear capabilities that could be used to conduct first strikes against China's nuclear deterrent and blunt Chinese retaliatory capability.

The United States' main concern is not preemptive Chinese nuclear use but rather the perception that China will not eschew the use of force in territorial disputes with its neighbors, several of whom are U.S. allies or partners. In this context, the United States is worried that China's increasing cyber, conventional, and nuclear capabilities are intended to prevent the United States from defending its allies.

The Chinese and U.S. concerns are both negative, meaning that each country is focused on avoiding adverse outcomes caused by the other side's behavior. In positive terms, strategic stability means that neither would initiate military conflict against the other (or against their allies), but that if conflict did occur neither side would think it feasible to undertake a first strike against the other's strategic forces.

The differences in these threat perceptions and approaches to stability are complicated further by the significant disparity in the two countries' nuclear arsenals. The United States has long defined its nuclear requirements in terms of balancing Russia. Together, the United States and Russia possess more than 90 percent of the world's total stockpile of nuclear weapons. But U.S. officials have noted in recent times that China's arsenal is rapidly growing and on track to expand over the coming decade. They express concern that this trend might have adverse operational implications.

Generally, however, U.S. concerns tend to focus more on China's broader strategic behavior and intentions. U.S. observers note with alarm that China's massive conventional buildup and force projection capacity is designed to dissuade the United States from coming to the aid of its regional allies and neutralize its operational conventional capacity to do so. This, in turn, reinforces U.S. fears that China desires to unilaterally change the status quo in regional disputes—by force, if necessary—while striving to blunt the United States' capacity and will to intervene. U.S. experts and politicians also express serious concern that China is behaving aggressively in several additional domains. Former secretary of defense James Mattis claimed in the 2018 U.S. National Defense Strategy that "the most far-reaching objective [of U.S. strategy] is to set the military relationship between our two countries on a path of transparency and non-aggression."[22]

In this deteriorating security context, the oversight over cyber operations that might intentionally or unintentionally affect NC3 is a growing concern. Cyber operators in both countries might not fully appreciate the intricacies and sensitivities of NC3 systems; only those at the very top of the hierarchy may have both the access and authority to review such operations. It is against this backdrop that U.S. officials assume China would undertake cyber attacks that could—whether intentionally or unintentionally—weaken U.S. NC3 systems, for example against early-warning satellites. They fear that China's highly siloed and compartmented governance of military and intelligence capabilities and operations, including in the cyber domain, would preclude its top-level political leaders from providing rigorous oversight. This concern is especially profound among U.S. experts who have been part of the U.S. government's effective cyber interagency policy vetting processes but see no indications that China is employing anything similar in the nuclear, conventional, and cyber domains.

Broadly speaking, as China-U.S. relations evolve toward intense great-power competition, they seem to display the classical security dilemma.[23] Each side feels endangered by the other and takes actions to secure itself. The other, viewing these actions as counterproductive, destabilizing, or even escalatory, then responds. Both sides lack confidence in the other's willingness to maintain strategic stability, restrain its actions, or build mutual trust. This problem has intensified in recent years as

trade competition, concerns about cyber-related behavior, ongoing military buildups and coercive actions in regions of concern, and general political confrontation have alarmed both sides. The coronavirus pandemic has brought the bilateral relationship to a low point not seen since 1989.

However, strategic stability would bring significant benefits to both countries and the world at large. China and the United States objectively share common interest in seeing the continued functioning of the global digital economy and in avoiding general military conflict. Over time, they could define certain types of cyber operations as mutually off limits and then identify ways to bolster each other's confidence that such limits are being respected (as we explore in a later section).

The Cyber Dimension

Cybersecurity has figured prominently in China-U.S. relations since 2012. The two countries have wrangled over a number of cyber and cyber-related issues, including internet governance, freedom of speech, online theft of commercial secrets, massive cyber surveillance, and cyber attacks. The stability of their cyber relations has been further disrupted by mutual accusations, such as Washington's blaming of China for cyber espionage for commercial purposes (including the APT1 report[24]) and national security objectives (the U.S. Office of Personnel Management incident[25]), and Beijing rebuking U.S. cyber operations against China and Chinese companies, as revealed by Edward Snowden. These have poisoned the two countries' attitudes toward each other in the security and commercial realms, leading to diplomatic, political, and economic confrontations and conflicts. These tensions have been further inflamed by widespread suspicions and allegations that both countries have manipulated supply chains or cryptographic equipment to introduce back doors into products and services.

That said, the two sides maintained dialogue and cooperation until recently. During the 2013 meeting between then U.S. president Barack Obama and Chinese President Xi Jinping in Sunnylands, the two agreed to collaborate on cyber issues through a bilateral working group. Another meeting between the two leaders in 2015 resulted in a mutual commitment to not conduct or knowingly support cyber-enabled theft of intellectual property, as well as the establishment of a high-level dialogue on combating cyber crimes. In 2017, the two sides set up a mechanism for law enforcement and cybersecurity dialogue.[26] Yet, these hopeful efforts have been frustrated by various actions and reactions between the two countries, as well as allegations (especially in the United States) that the Xi-Obama understanding is no longer being faithfully implemented. Today, there are no meaningful discussions on cybersecurity. There are not even any understood norms of con-

duct, whether explicit or tacit, to constrain all actors engaged in intelligence collection and offensive cyber operations. Although no massive conflicts have occurred between China and United States in cyberspace in the intervening months and years, friction has become incessant and increasingly intense.

Each side's growing cyber capabilities now assume special importance in its overall homeland security, intelligence, and military posture. The capabilities are symbols of state power and have practical operational significance. Cyberspace is now a leading domain for intelligence collection, covert operations, military encounters, and even outright warfare. Cyber operations are central not only in a conflict but also during the buildup to conflict and in peacetime. Cyberspace is increasingly a medium for influencing cognition and behavior as well as affecting physical capabilities. The net effect is that cyber capabilities profoundly influence strategic stability and, in particular, nuclear stability.

The lure of cyberspace seems almost irresistible. Cyber tools are less expensive to acquire and operate than conventional weapons. They offer huge potential geographic coverage, economies of scale, and force-projection capabilities. They are also largely of a dual-use nature, emerging naturally from commercial applications at little or no additional cost. Cyber operations are typically highly secretive. This avoids the scrutiny associated with other types of operations and presents options for plausible deniability. Cyber operations are subject to fewer formal legal constraints and moral inhibitions. Despite the risks of spurring escalation in other domains, cyber operations are still appealing because they are often opaque and do not necessarily cause obvious physical damage. These features could mitigate fears that adversaries will respond by escalating across domains. Many of these benefits are growing as the human operating environment is becoming more and more digitized.

We do not know details of either China's or the United States' cyber capabilities to attack the other's NC3 systems or defend its own. But the United States openly acknowledges possession of formidable offensive cyber capabilities, explains their purpose, and publicly discusses some of its doctrine. It also has procedures in place to manage their use with clear lines of authority, review, and accountability, although extensive delegation of authority to employ such capabilities seems to have taken place under former president Donald Trump's administration. The U.S. government believes that many other countries already possess or are actively developing offensive military cyber capabilities; naturally, China is at the forefront of this group.

China, on the other hand, is publicly wedded to the peaceful use of cyberspace and steadfastly declines to discuss offensive cyber capabilities and relevant doctrines. It argues that the key to stability in cyberspace is for countries to renounce using cyber tools to commit aggression and interfere in the internal affairs of others. China's recent National Defense White Paper does state that its armed

forces will "accelerate the building of their cyberspace capabilities, develop cyber security and defense means, and build cyber defense capabilities."[27] The document describes China's military cyber units and capabilities as defensive in nature, designed solely to defend and react as "Strategic Support." Chinese leaders' professed desire to avoid arms racing and war in cyberspace is similar to China's long-standing approach to renounce first use of nuclear weapons as well as militarization and confrontation in outer space. These positions all differ from those of the United States.

The contrasts between these approaches create a circular problem that prevents mutual understanding, let alone trust. Without mutual understanding, it is difficult for the two sides to conduct meaningful bilateral conversations on strategic stability in cyberspace. In turn, the lack of such dialogue makes mutual understanding and confidence harder to achieve. This circular problem is especially grave when it comes to threats that cyber incidents may pose to NC3 architecture. Such threats could lead to escalation beyond levels that national leaders intend.

In this context, it is especially important to note China's heightened concern over recent changes to U.S. cyber strategy and policies. China views with alarm official documents and public statements that signal a shift in U.S. strategy from a restrained, reactive posture in cyberspace to one of more active, day-to-day contestation through "persistent engagement" with U.S. adversaries.[28] The U.S. Department of Defense's cyber strategy emphasizes "defending forward" to "disrupt or halt malicious cyber activity at its source."[29] Alongside these doctrinal changes, a presidential directive in 2018 reportedly eased the approval process for offensive cyber operations that fall below the level of "use of force."[30]

U.S. defense officials assert that "defending forward" does not fundamentally change the defensive purpose of their activity. Rather, the concept reflects evolving ways of countering malicious cyber and information operations below the level of armed conflict. They describe "defending forward" as including information sharing with partners, not just operations targeting foreign cyber actors.[31]

What these changes mean in practice remains to be seen. But vague definitions of central concepts and mixed messages from U.S. officials leave open the possibility that this new strategy involves deep routine penetration of Chinese (and other) systems. This would reinforce the Chinese view that the United States is becoming more aggressive in cyberspace (as in other domains). China worries that U.S. actions intended to deter and defend could actually increase the likelihood of cyber crisis and force the two sides to prepare for worst-case scenarios. This would mean both sides expanding, intensifying, and accelerating assertive cyber operations to gain a sense of security in cyberspace. The United States' use of "left of launch" cyber operations against North Korea's missile systems is illustrative. Although the target is a physical system rather than a cyber capability, such operations

nevertheless reflect the attractiveness of prevention and preemption in cyberspace. Such operations influence Chinese perceptions of what "defending forward" otherwise referred to as "persistent engagement" might mean.[32]

U.S. decisionmakers agree that cyberspace presents distinct challenges to China-U.S. relations but identify an altogether different set of challenges than their Chinese counterparts. The differences in perspective between the parties seem deeply rooted. Whereas China is concerned with aggressive U.S. cyber policy and doctrine, U.S. analysts emphasize larger disagreements about cyberspace, like how international law applies and what constitutes armed attack in this domain. Americans also lament the absence of common understanding on the rules of the game for cyber confrontations. Chinese observers acknowledge these areas of disagreement but believe they are not highly relevant to potential China-U.S. negotiation on maintaining strategic stability in cyberspace.

U.S. suspicions about Chinese sincerity are heightened by their perception that China and Russia have formally aligned their stances on cyber diplomacy. This has led U.S. observers to identify China with what the United States considers Russian duplicity.[33] From their perspective, Russia has called to ban warfare in cyberspace while itself engaging in extremely aggressive and deceitful cyber conduct even during peacetime. This includes Russian espionage, information operations, and physical disruption and destruction against multiple states. Since China publicly subscribes to the same formal position as Russia, U.S. experts worry that China could act similarly.

Against this backdrop, some U.S. experts consider China's reluctance to talk about its cyber capabilities and governance policies as a sign of bad faith. They suspect that it is designed to conceal Chinese intentions (or at least preparations) to conduct cyber attacks against the United States. They are also concerned that China's reticence hides a deficiency in internal deliberations over the development and employment of cyber tools and political oversight over their employment. U.S. specialists fret that Chinese operators have considerable leeway to conduct more frequent and unintentionally destabilizing use of cyber capabilities against the United States. U.S. experts thus maintain that an official admission of Chinese possession of an offensive cyber capability and articulation of the doctrine governing its use are essential for any meaningful bilateral dialogue on mutual restraint and stability.

In addition, U.S. officials consider it difficult to imagine how the two sides could develop a modicum of trust if major cyber-related concerns are taken off the table. For years, U.S. officials and experts have decried China's restrictions on the free flow of information—most recently, China's implementation of a new cybersecurity law that will have "significant adverse effect" on trade and commerce.[34] China's domestic information policy and its multiyear economic espionage campaign

prompt similar alarm—a view repeatedly echoed in statements by senior members of U.S. congress of both parties—as revealed by U.S. Department of Justice indictments and the Mandiant report,[35] for example. In recent years, U.S. officials have also repeatedly expressed serious concerns about the intimate and opaque relationship between the Chinese government and leading Chinese technological companies (though they have not yet provided public evidence to support their claims). They suggest that these government-corporate connections pose national security risks not only for the United States but for other nations as well.[36]

Chinese officials, meanwhile, have condemned the United States for conducting large-scale espionage via cyber tools,[37] rejected U.S. allegations about the relationship between Chinese government and technological firms, and accused the United States of smearing Chinese information and communications technology (ICT) companies without solid evidence and unilaterally cracking down on Chinese companies by promoting the Clean Network Initiative.[38.]

China also emphasizes that mutual trust must be established before progress can be made on transparency and other specific issues. To them, asking for information about capabilities without trusting the other side's intentions is just another form of spying. Some information could be exchanged, but no one would be willing to view it as trustworthy or to provide particularly meaningful details.

Chinese experts have also repeatedly expressed disappointment that the United States continues to take hostile actions against China—such as charging Chinese military officers and arresting Chinese scientists—while simultaneously urging China to participate in comprehensive bilateral dialogues. These researchers and others think such U.S. actions have sent mixed and confusing signals and will only erode the basis for trust that is necessary for a meaningful dialogue.[39] For example, the cyber security working group established in 2013 to conduct dialogue between the two militaries was abandoned after the United States indicted five Chinese military officers. They further note that "any lack of mutual trust (in the military and intelligence spheres) will probably lead to low-intensity conflicts."[40]

These fundamentally conflicting views on the nature and mechanics of bilateral dialogue have long obstructed progress in most areas of tension, not only cyber issues. While the United States generally prefers to divide differences into concrete issues and then start to build trust by addressing the most urgent and thorny problems, China believes there can be no meaningful progress on these practical issues if trust doesn't already exist. China strongly advocates focusing instead on strategic intentions, believing that all other concrete problems can be solved if mistrust is overcome.

The issue of trust between China and the United States undoubtedly runs far wider and deeper than the cyber domain alone. Nevertheless, it seems especially important to address here because of the technical and operational incentives to use offensive cyber capabilities at the very beginning of conflict when targets are most vulnerable and one's own assets would be most potent. This is a variation on the classic "use it or lose it" situation. Furthermore, it may lead to arms race instability or even crisis instability. The lingering mistrust over this security dilemma will otherwise make both countries' officials and experts view the other's behavior through suspicious eyes and interpret changes of policy and posture as aimed at coercion and pre-emption.

Cyber-Nuclear Risks: Scenarios of Particular Concern

Against this background, each side worries about the other military's incentives to conduct cyber operations that could threaten NC3 systems. Three scenarios pose the most pressing concerns.

First, preventive or preemptive actions might be taken in cyberspace ahead of a conventional confrontation. Such actions could inadvertently affect nuclear assets and their nuclear command and control infrastructure. Second, cyber action may occur once a conventional conflict has begun. This might be intended to prevent nuclear escalation but could unintentionally bring it about. Third, the very threat of cyber operations can produce acute anxiety about the safety, survivability, and reliability of nuclear forces, thereby triggering higher states of alert and other defensive measures. These may cause accidents and errors or be misinterpreted by the other side as offensively motivated. All these scenarios could produce dire unintended consequences.

There are compelling reasons why states—especially nuclear-armed states—might want to conduct cyber operations against an adversary's NC3. Forward cyber operations can generate valuable intelligence and provide timely early warning of nuclear (or non-nuclear missile) attack, as well as reassurance that preparations for such attacks are not underway. In fact, high granularity intelligence may also prove necessary to sort out whether a nuclear alert, if detected, is defensively or offensively oriented.

Some states may also consider cyber operations conducive to deterring an adversary's use of nuclear weapons. By penetrating NC3 in a way that can be detected and/or knowingly disclosing relevant information afterwards, cyber operations might erode the adversary's confidence in the availability,

integrity, and confidentiality of their system. Even if the exposed vulnerability can be readily fixed, the adversary will worry that another one already exists or could be found and exploited. The adversary may then be dissuaded from taking threatening nuclear steps.

In extremis, cyber operations can also degrade an adversary's capacity to use its nuclear weapons. If targeted at the tactical level, cyber operations to degrade nuclear weapons systems would not necessarily be as escalatory as a nuclear or conventional attack on those same systems.

Cyber capabilities that enable attacks on NC3 systems are largely interchangeable with capabilities to gather intelligence on these systems. The deep reconnoitering of systems from within is a necessary precursor for attacking them. As one veteran cyber operator put it, "when you are in, you are in"—and once you're in, any number of things can happen.

This makes it very difficult to interpret the motivations behind cyber intrusions. The designers and operators of these tools will rarely be completely certain of their technical effects, let alone how they shape the perceptions of those on the receiving end. The operators and leaders of the targeted state's nuclear apparatus will likely be even less certain in their assessment of an intruder's motivations. They will want to know quickly: are these naturally occurring technical failures and mishaps, accidents, or adversary attacks? And, if the latter, who actually (and not merely apparently) launched them, who authorized them, what systems were impacted, how have they been impacted, what was the purpose, and was it in fact intended to cause still greater damage? Even lengthy investigations rarely produce certain answers to all these questions.

Neither side will be able to fully appreciate the impact of employing such capabilities on both core and auxiliary systems, let alone on systems that the attacker did not know were involved in supporting nuclear missions. (This is very likely to occur, given the extreme secrecy surrounding nuclear systems.) If, as some believe, significant asymmetries exist between the two countries' capabilities to detect and correctly attribute cyber operations in their systems, the rationality and quality of decisionmaking will be further complicated.

These uncertainties are compounded by possible divergences in how thoroughly each country has integrated knowledge, operational management, policy oversight, and decisionmaking among the agencies that develop and operate cyber capabilities and nuclear forces. As described earlier, cyber operators may not adequately know, let alone understand and appreciate, adversaries' complex and highly classified NC3 systems. Thus, they may not be able to accurately inform their leaders of the potential consequences of proposed or conducted cyber operations.

Major differences between the structure and doctrine of U.S. and Chinese nuclear forces also affect the vulnerabilities of their respective command and control systems. These vulnerabilities, in turn, influence whether and how China and the United States might be tempted to target each other's NC3 systems, as well as how they would defend against such threats.

If China perceives that the United States is seeking "left of launch" cyber capabilities against China's nuclear deterrent, China could perceive any cyber intrusion into its systems as a deliberate attack by the United States on its nuclear deterrent—even if the actual source and intent behind the intrusion remain uncertain. China may even feel pressure to engage in cyber espionage to try to understand what the United States could be planning. Similarly, if the United States detected cyber espionage, U.S. officials could find it much more threatening and aggressive than Chinese officials intended. Finally, the vast differences between China's and the United States' nuclear forces and doctrines impairs each side's understanding of the other's NC3 systems. Neither side may understand well how the other's NC3 is integrated with conventional forces. This could increase the risk of cyber operations inadvertently impacting extremely sensitive systems.

Diverging perceptions of the balance of cyber capabilities between the United States and China may exacerbate these risks. Chinese experts appear to strongly believe that China is weaker, with more limited power in a potential cyber conflict. This perception might make China more anxious about its ability to detect, attribute, or thwart a potential U.S. intrusion into its NC3. The current expansion and diversification of China's nuclear forces could strengthen its second-strike capability, which could be stabilizing. On the other hand, new nuclear forces could also end up increasing the vulnerability to adversary cyber penetration, adding to anxiety instead of reassuring Chinese leaders.

Chinese counterparts believe that U.S. officials understand their thinking on this issue. China's smaller nuclear arsenal is not suited for conducting first-use counterforce strikes on the United States—whether or not Chinese cyber attacks could slow or impede U.S. nuclear operations. Chinese cyber operators further assume that U.S. officials fully understand that China has no intention of neutralizing the U.S. nuclear deterrent. Thus, China may underestimate the possibility that cyber espionage, for example, could unintentionally raise risks of escalation. This risk is greater still if U.S. defense analysts don't agree that China is much weaker in cyberspace (or truly committed to its no-first-use policy). Because U.S. analysts have observed what they think are aggressive Chinese actions in cyberspace and beyond, the United States would consider Chinese cyber operations in its NC3 system a grave threat.

A further potential source of instability and conflict escalation arises from the increasing entanglement of nuclear and non-nuclear assets.[41] Over the next few years, as the United States invests heavily in improving its overall command and control capabilities, it will likely integrate capabilities that used to be held and operated separately by each military service. At least some functions of NC3 will probably be fused into a multi-domain command and control. The U.S. Department of Defense has embarked on a broad effort to establish Joint All-Domain Command and Control (JADC2), which would reportedly link and integrate sensors and communications across all services and in all warfighting domains. While this concept is still under development, U.S. defense officials have indicated that JADC2 will be "intertwined" with NC3.[42] This raises concerns that NC3 capabilities would then become even more difficult for adversaries to distinguish from non-nuclear ones. China may already be using one shared command and control system for its conventionally armed missiles and its nuclear-armed missiles. The People's Liberation Army Rocket Force (formerly the Second Artillery Corps) is widely believed to be dual-functioned. At least some Chinese early-warning assets, including its over-the-horizon radars, may contribute to both nuclear and non-nuclear operations.

It is impossible now to know with certainty what the implications of conventional-nuclear entanglement are or could be for China-U.S. cyber-nuclear dynamics. But representatives of the U.S. military services, nuclear and cyber commands, and civilian officials might not have a clear understanding, let alone full appreciation of how entanglement could affect China's threat perception. Similarly, their Chinese counterparts may not be fully aware of how their existing joint command and control affects U.S. perceptions and plans. The more nodes a network has the more potential cyber vulnerabilities it has—and the more difficult it becomes to determine exactly what capability an adversary is endeavoring to disrupt. In the interim, both countries have become increasingly reliant on multipurpose assets like satellites that provide communication and early-warning support for both conventional and nuclear forces.

In sum, there are many ways cyber operations could go wrong. Even the most sophisticated, finely targeted cyber operations may produce unintended effects, including spreading to other systems and causing collateral damage.[43] Potential unforeseen ripple effects are not confined to technical systems. Corrupting data or systems and the creation of uncertainties about control over nuclear forces could create confusion or destabilizing dynamics in the minds of decisionmakers. Those on the receiving end of cyber intrusions face extreme challenges assessing their origins, intentions, impacts, and implications in real time. Distinguishing technical malfunctions from cyber attacks, let alone reliably attributing them, is a time-consuming exercise. This profound strategic mistrust means that, in a crisis or conflict, virtually *any* cyber incident impacting nuclear systems could produce anxiety, confusion, alarm, and extreme decision-making pressure on responsible authorities.

The primary purpose of this research is neither to explore all the possible permutations nor simply to describe the problem. We seek to suggest practical steps to reduce and manage these risks to serve the common interest in strategic stability. With this in mind, we identify categories of scenarios where cyber operations in and on nuclear NC3 (intentionally or unintentionally) could lead to arms racing, crisis escalation, or even nuclear conflict. Nearly infinite variations on these scenarios can be imagined. Our aim is more simply to identify factors that would be most destabilizing, so that we can then highlight the most worrisome risks to stability that China and the United States could want to reduce. We then turn to our main purpose—exploring possible ways to reduce such risks.

Functions of NC3

In order to decide on which scenarios to focus, it is helpful to define the basic functions that any NC3 architecture can serve.[44] According to our understanding, the functions are to:

1. guarantee effective monitoring and exclusive control at all times over all nuclear forces and strategic operations;

2. support decisionmaking, planning, and operations in all scenarios;

3. provide timely warning of imminent attack;

4. supply situational awareness to the various command levels;

5. assure effective and secure communications to and from national command authority;

6. accommodate and support all required maintenance, upgrade, safety, and surety operations;

7. withstand all efforts to undermine or subvert the reliable transmission of information and guidance between and across command levels; and

8. sustain high standards of safety, security, and secrecy commensurate with the sensitivity of nuclear weapons.

Digital security incidents (or attacks) are usually categorized as affecting the "AIC triad," which means the availability, integrity, and/or confidentiality of hardware, software, networks, and data. In this paper, we focus on the potential effects of incidents affecting the availability, integrity, and confidentiality of NC3 components, products, and services. They could include one or more of the following (which are not mutually exclusive):

1. communications are cut off or disrupted between national command and other elements of NC3, between early-warning systems and other elements of NC3, or between NC3 and the operational units, diminishing their responsiveness and accountability to National Command Authority guidance;

2. the confidentiality of data is compromised (potentially at all levels), possibly skewing decision-making and putting nuclear forces at risk;

3. the integrity of data used for warning, decisionmaking, and response—as well as for operational control—is compromised and manipulated (potentially at all levels), possibly undermining situational awareness and distorting warning and response processes;

4. delivery mechanisms or platforms are disabled or distorted;

5. trust in the reliability of systems and processes, perhaps even in the entire nuclear arsenal, is shaken, causing heightened alarm and affecting strategic and operational choices and responses;

6. the discovery of an attack on these systems triggers retaliation or response in kind or in escalation against the suspected perpetrator; and

7. misplaced complacency occurs (if attacks are not discovered, or if attacks are discovered and defused ahead of time).

Elaborated Scenarios of Special Concern

As discussed earlier, deliberate cyber efforts to degrade, disable, and/or compromise NC3 would undoubtedly pose serious risks. The blurred lines between cyber espionage and attacks, the potential contagion and cascading effects of attacks (beyond those that were originally targeted or compromised), and the persistent uncertainty about the identity of the perpetrator and their intentions all make cyber operations likely to inadvertently create highly destabilizing effects. Four types of scenarios are worth discussing here.

The first type involves **cyber espionage collecting data on and inside the core** of an adversary's NC3 system. When detected, the targeted country may interpret an established foothold in its NC3 and the reconnaissance and exfiltration of information from it as a prelude to an impending armed conflict, which could precede an attack on its nuclear forces.

The second type similarly involves **cyber espionage** but, in this case, it occurs **in dual-use systems** or other elements supporting or connected with NC3, perhaps without the perpetrators (or target government) having full appreciation of their nuclear nexus. Potential targets include dual-use C3 systems, especially early-warning assets, electricity supplies, or other auxiliary systems supporting NC3. Though not as sensitive as the first scenario, such operations can be similarly interpreted as an indication of and preparation for an impending attack in general and on nuclear forces in particular.

The third cluster of scenarios involves **cyber attacks directed at dual-use** (conventional alongside strategic) **NC3 systems or auxiliary systems** supporting or connected with NC3 but without any intention to affect their nuclear functionality. Potential targets include the same dual-use C3 systems listed in the second type of scenario. Regardless of the perpetrator's intent, such operations could affect the targeted state's nuclear functionality, or at least be interpreted by the target as having such objective.

The fourth type of scenario involves cyber-related phenomena where the combination of serious suspicions about the intentions of the other party and apprehensions about the vulnerability of one's own NC3 to adversary cyber attacks result **in overreaction and the escalation of a crisis.** Technical malfunction, misdiagnoses of an accident, or human error may all be attributed (at least temporarily) to a cyber attack or trigger a false warning of an incoming missile attack. As artificial intelligence algorithms are incorporated into NC3, the prospects of these scenarios increase. States may react to anxiety about their nuclear forces' vulnerabilities by adopting policies that produce even greater risk of crisis instability—such as "launch on warning" or pre-delegation of launch authority to local forces.

Potential Consequences of Real or Perceived Cyber Operations Against NC3

Cyber operations could intentionally and directly produce strategic consequences for good or ill to the United States, China, or both. Even the anxiety over or anticipation of such operations, whether or not they occur, could produce strategic consequences. So, too, could China or the United States mistakenly thinking operations are being directed against them, or misinterpreting accidents or operations that are occurring.

The distinctive features of cyber operations make all these scenarios possible. It is highly unlikely that the perceived targets of cyber operations would not be worried at all, since nuclear safety and security are at stake. Thus, our focus here is on potential consequences if the target side feels compelled to take countermeasures.

Of course, it is also possible that such operations would deter the adversary from responding in escalatory ways. That possibility is what drives adversaries to create the threats we are addressing, and what makes it difficult to persuade them to entirely rule out such actions. Since individuals and organizations that practice deterrence intend to prevent war (or, if war occurs, its escalation), yet at the same time also deem it necessary to prepare for situations in which deterrence efforts fails, they are especially reluctant to forego offensive capabilities that they deem expedient for such scenarios. In order to encourage considerable restraint when undertaking such activities—and extreme prudence if and when they do elect to engage in such activities—it is necessary to understand the risks posed by such intrusions. Their potential harmful consequences could dwarf their perceived deterrence benefits.

Four broad types of strategically worrisome consequences of these scenarios emerge:

1. **Nuclear conflict** could be caused if the target state observes (correctly or otherwise) cyber operations against their NC3 and conclude that they must quickly unleash their nuclear weapons in order to avoid losing the capacity to do so later. A false reading of an incoming attack due to malfunction in the early-warning and communication system could unleash the same scenario.

2. **Inadvertent or accidental use of a nuclear weapon** could result from a system failure, wherein a disabled NC3 prevents commanders from withdrawing pre-delegation of authority for nuclear release, reversing escalatory activity orders, or stopping an unauthorized use of nuclear weapons. These consequences could also ensue if a rogue actor gained access to NC3 or nuclear forces.

3. **Crisis escalation** could occur in multiple ways. The effects of cyber operations could propagate unintentionally from a non-nuclear target to NC3. The intentions behind cyber operations could be misattributed or misperceived, producing the mistaken perception that one's nuclear forces are under attack or adversary nuclear weapons have been launched against one's state. Technical malfunction or human error could lead to a cyber operation being improperly attributed to an adversary when it was actually an error, an accident, or a malfunction. Finally, decisionmaking could be degraded due to lost confidence in critical systems or information that in fact has not been compromised or, conversely, erroneous confidence in systems or information that have been.

4. **Long-term destabilizing impacts** would most likely include arms racing and ensuing crisis instability. Another possible consequence is mounting pressure to compensate for lost confidence in NC3 by, for instance, pre-delegating launch authority or incorporating artificial intelligence into analysis and decisionmaking. Perhaps the greatest adverse effect would come from the loss of confidence in the reliability of one's nuclear deterrent.

In our view, inadvertent or unintentional effects comprise the most important category of risk that the United States and China could address in the near term—though they do not pose the greatest challenge to cyber-nuclear stability between the two states. All these risks are made more likely and difficult to redress because of the potential for third-party actors to sow confusion and exacerbate crises, the challenges of attribution and the implications if two adversaries have asymmetrical attribution capabilities, and inherent difficulties that attackers and targeted states have in assessing effects of cyber operations in advance or real time.[45]

Possible Measures to Enhance Strategic Stability and Mitigate Cyber-Nuclear Risks

Our discussions have produced a consensus that the United States and China could and should endeavor to mitigate risks and enhance stability associated with the cyber-nuclear nexus. Intensified distrust between the two countries does not necessarily prevent them from cooperating to build confidence to prevent the most destabilizing sorts of actions in and through cyberspace. Both countries share the desire to avoid inadvertently sliding into armed conflict and are committed to averting escalation toward nuclear war, although the United States does not rule out first nuclear use in extreme circumstances. Thus, many strategists and nuclear/cyber experts believe that neither the United States nor China would benefit from jeopardizing the capacity of the other to effectively command its nuclear forces in all but the most extreme circumstances (and, perhaps, not even then).

We consider several types of measures that the United States and China could undertake unilaterally, reciprocally, and/or bilaterally to enhance stability and trust in this domain. These steps include broad measures to enhance strategic stability between the two countries; measures associated with their cyber postures, as well as the structures and capabilities of their nuclear weapons arsenals; and concrete steps to directly enhance the robustness and resiliency of their respective NC3 architecture against cyber threats. The prospective policies, norms, and various forms of communication listed in this section aim to ease acute concern and enhance trust.

Assured Decision-making Procedures for Cyber Operations

As we described in the introduction to this paper, cybersecurity involves actors, technologies, and phenomena that cross multiple sectors of national and international economies and governments. Coordinating decisionmaking across all these sectors is usually a difficult process. Moreover, operators and decisionmakers at various levels may not fully appreciate or anticipate how their own cyber operations may spill over and affect other domains. Officials may not understand why and how their own capabilities or actions seem threatening to others. They may not be able to evaluate the chain reactions that are likely to occur as others respond to their action. In such a complex technological and political-bureaucratic environment, it is easy for everyone to exaggerate the threats that others pose.

With or without convergent definitions and understandings of cyber stability, the United States and China could benefit themselves and each other by adopting certain unilateral approaches to cyber policy and decisionmaking. The inherent risks and uncertainties of cyber operations mean that the self-interest of each country, as well as their mutual interest, depends on subjecting cyber operations to robust oversight and risk management. This can be done in a manner that is tailored to the unique circumstances and governance arrangements in each country and satisfies secrecy and compartmentation requirements while allowing for assessment and control procedures.

We recommend clarifying oversight at five levels:

1. **Domestic and foreign policy oversight** by competent national authority, so that adequate consideration is given to the potential reactions of domestic and/or foreign actors if they discover one's cyber operation against them.

2. **Technical oversight** that includes a "technical gain versus loss" assessment, which addresses the unintended consequences if the technical capability used in an operation is discovered and used against other targets including in one's own territory. Such oversight also should provide assessments (at low, medium, and high assurance levels) that the capability will produce technical outcomes or effects as intended and not produce unintended consequences such as escalation or cascading effects.

3. **Operational oversight** with appropriate responsibilities, accountability, and command and control procedures that verify positive control within an authorized chain of command.

4. **Intelligence oversight**, including an "intelligence gain versus loss" assessment that addresses the consequences of exposure and potential loss of intelligence sources, methods, and resulting future insights if the cyber operation or capability is discovered or revealed.

5. **Legal oversight**, which includes two types of legal review that provide an assessment both for the capability and for the operation as it applies to either the international law of armed conflict or other applicable domestic and international laws and agreements.

Implementing oversight arrangements like these would unquestionably reduce risks of ill-conceived cyber operations. If such oversight procedures were applied to cyber operations that could affect NC3, they also would enhance stability: well-briefed senior leaders presumably will strive to reduce any prospect of causing escalation through mistakes or ignorance, and then having to explain what happened to political rivals, citizens, and the world. This caution-inducing benefit would arise from the unilateral arrangements discussed here, which could be undertaken in total secrecy.

Additional benefits could accrue from engaging the United States and China in bilateral dialogue on these issues. Optimistically, such dialogue could help convince officials on both sides that meaningful discussions could be sustained without compromising secrecy. This could facilitate the creation of forums for officials and experts from both countries to exchange perspectives on these issues. Each side could, at minimum, share with the other its concerns and inform them of the internal oversight arrangements they have adopted. The key is to reassure each other that cyber operations that could potentially affect NC3 systems would require very senior-level approval.-

Creating a More Stable and Less Vulnerable Strategic Context

The United States and China are both taking steps to modernize their nuclear architecture and forces, including their NC3 systems. Among other things, they seek to enhance the security, reliability, and resilience of their NC3 systems in order to bolster their entire deterrents. These efforts pursue two complementary logics and objectives. The first is *robustness*—steps to "immunize" nuclear arsenals and NC3 from a cyber attack, including isolating dedicated nuclear systems and hardening infrastructure and systems. The second logic and objective is *resiliency*—measures and capabilities to allow for smooth and swift recovery from a cyber attack. Examples could include providing backup communications channels and command posts, and adding redundancy in power supplies and other essential supplies.

In this context, it is worth recalling that there is an inherent asymmetry between the two countries' modernization efforts. For China, the primary driver may be perceived threats from the United States. For the United States, however, the primary (though not exclusive) concern in the nuclear domain is Russia. Regardless of intent, China will not find U.S. modernization very reassuring. China believes that current and planned enhancements to U.S. forces and NC3 go well beyond cybersecurity measures and improve the United States' operational capacity to conduct preemptive nuclear operations against China. Such operations could disable or destroy China's nuclear deterrent,

or blunt China's capacity to execute ordered nuclear retaliation. As one Chinese participant noted, "Any resiliency efforts with the aim of offsetting or decreasing the nuclear capability of the other side will be viewed as a threat or having the potential of leading to instability. We should encourage resiliency measures with the aim of enhancing one's own cyber defense. They can include isolation, enhanced supply chain security, backup." This partly explains China's reluctance to dialogue—in this traditional view, ambiguity about Chinese capabilities and strategies helps offset U.S. advantages.

Whether or not meaningful sustained dialogue on these issues occurs, it is worth considering the potential risks and benefits of various ways in which China and/or the United States could adapt their nuclear forces, doctrine, operational planning, and NC3 systems to make them more robust and/or resilient without in the process triggering retaliatory steps by the other party.

Increasing the number, diversity, and modes of deployment

This option pertains mostly to China because the U.S. nuclear arsenal is scaled to contend primarily with Russia. Having agreed in February 2021 to extend the New Strategic Arms Reduction Treaty for five years, the United States and Russia will not increase the number of their deployed strategic nuclear weapons for at least five years. There is also no apparent sign thus far that concerns about cyber attacks on their NC3 are the ones causing them to increase the variety of their nuclear weapons or their modes of deployment.

China has a significantly smaller nuclear force that relies mostly on ground-based delivery systems but is growing its presently modest submarine-based ballistic missile capability. Chinese leaders could decide for a variety of reasons (including in response to growing U.S. missile defense capabilities) to increase the overall number of their nuclear weapons and invest much more in air- and (longer range) sea-based delivery. Such decisions might enhance their confidence in the survivability of their nuclear second-strike capability. But it is unclear whether they would significantly decrease the vulnerability of the overall nuclear deterrent to cyber attacks and, if so, to what extent. As noted above, much depends on how such changes would be executed in terms of supply chains and quality control, and how these will be perceived by the United States.

Accordingly, participants suggested that some types of prudent Chinese responses could be recognized as stabilizing. Examples include strengthening the security and safety of its nuclear weapons systems and the resilience of its NC3 by lowering the scale and level of NC3 systems' dependence on cyber elements; introducing more backups for the auxiliary systems (for example, power supply); bolstering national innovation and acquisition to increase their self-reliance regarding the supply of key ICTs; and maintaining relatively a low level of NC3 access to the internet.

Lowering restraints on readiness and nuclear use

The United States has sought capabilities to be able to conduct preemptive cyber, conventional, or nuclear strikes on adversary nuclear forces, doubting that China will uphold its no-first-use pledge in an actual conflict. We and other participants in this project assess that lowering restraints on nuclear use will exacerbate instabilities and increase risks of nuclear use and escalation, due to the possibility of flawed information and/or analysis. A better security strategy would be to strengthen restraints on premature or mistaken use of nuclear weapons. Improving the security, robustness, and resiliency of NC3 systems can help accomplish this.

Clarifying intentions and doctrines also could help modestly. For example, the United States has announced that it would consider employing any of the means at its disposal in response to cyber aggression, conceivably justifying a nuclear response to cyber attacks on its NC3.[46] This could reasonably be meant to enhance deterrence against cyber attacks and intrusions into critical assets, especially its NC3 apparatus. However, other countries worry that the United States could undertake a nuclear attack without accurate (or publicly shared) attribution. This could increase some states' motivation to harden or expand their nuclear arsenals, or to loosen restraints on use. It also could encourage them to conduct cyber espionage against the U.S. nuclear weapon system in order to detect when the United States might be preparing to conduct a preemptive attack. Such an incentive, in turn, could feed a vicious cycle, propelling Washington to adopt an even more aggressive deterrence policy.

We do not know whether the United States has, in fact, lowered the restraints on nuclear use in response to possible cyber threats. The possibility that it has done so concerns China, which could add to or detract from deterrence of conflict or avoidance of inadvertent escalation. This lingering uncertainty reinforces the case for a bilateral dialogue. The two sides can air concerns, perceptions, and intentions directly to each other, and demonstrate why the other's fears might be ill-founded or exaggerated. For example, one could contemplate reassuring the other that it is not going to take a number of steps to enable much quicker launches of nuclear weapons, such as mating nuclear warheads to missiles, pre-delegating launch authority to local commanders, or exercising launch-on-warning nuclear attacks. China and the United States might also consider hedging against cyber threats to NC3. For example, they could pre-delegate to military commands the authority to use nuclear weapons if command and communications systems are compromised. The perceived benefits, risks, and modalities associated with engaging in such action have been discussed elsewhere and will not be covered here.[47]

Development and deployment of new capabilities

It is conceivable that the development and deployment of new capabilities such as anti-satellite or space warfare weapons could also arouse concern about cyber-nuclear threats. The use of such weapons could undermine the integrity and reliability of NC3, either through cyber effects or other forms of disablement or destruction. We have already mentioned Chinese concerns that the United States' recent adoption of "persistent engagement" in cyberspace may undermine China's second-strike capability. Aside from the direct cyber threat to NC3, threats to (potentially dual use) space-based NC3 assets pose broader challenges—it would be prudent to address such issues in future Chinese-U.S. dialogue on strategic stability.

Another concern is about the application of artificial intelligence. If artificial intelligence is integrated into warning and command and control systems without great care, the risk of mistaken or otherwise unintended escalation could grow. New software, hardware, and/or practices that introduce novel vulnerabilities or potential flaws into systems would also increase the risk of accidental or inadvertent escalation. (To understand how measures to enhance robustness and resiliency of NC3 can exacerbate risks, consider the "Dead Hand" system that Russia developed, tested, and presumably even deployed in the late 1970s and early 1980s to enable the automatic launch of nuclear weapons under extreme circumstances.[48])

Mutual Commitments on Restraints

There are some scenarios where the United States and China could be highly unlikely to restrain cyber operations against NC3 and other command and control systems. If the leaders of either country have decided intentionally to enter a large-scale armed conflict and contemplate employing nuclear weapons, then they will be prepared to use them early in the conflict. Otherwise, they should expect to be confronted with this choice if they intend to fight an escalatory war. Fortunately, however, neither the United States nor China sees a potential lasting advantage in any such scenario. On the contrary, they both desire to pursue their competitive or conflicting interests without sliding into an armed conflict. With this shared strategic interest in mind, the primary risk that the two countries could address in the near term is the inadvertent escalation of conflicts leading to the use of nuclear weapons. They would thus be well advised to negotiate and/or unilaterally adopt measures to restrain their cyber capabilities and/or actions to threaten each other's NC3.

Of course, participants in our project acknowledge that tensions in bilateral relations cast doubt on the political viability of unilateral adoption of constructive restraining measures. Both sides may be motivated to demonstrate capabilities and willpower to deter the other from going too far. Both may feel that avowals of restraint could be seen, or at least politically presented, as a sign of weakness that would undermine deterrence and readiness. They may also fear such restraints will deprive them of

early preparations for a scenario in which the other changes course and plans to initiate or escalate conflict. Nevertheless, we believe that they ought to be seriously considered now so they could be implemented gradually as soon as political and strategic conditions allow.

Commitment not to intrude into core NC3 systems

We explored whether it would be desirable and feasible for the United States and China to formally commit to not conduct *any* cyber intrusion into core NC3 systems. Governments will naturally be inclined to continue to seek information on each other's nuclear forces. However, the United States and China could decide that intelligence operations to obtain information should not be carried out through cyber intrusions, whether they target core NC3 systems purposefully and directly or are designed to spread to the core NC3 from other systems. Additionally, they could pledge to take extra caution to prevent inadvertent propagation of effects to the core NC3 as a result of other cyber operations. Such a commitment could enhance stability and reduce the risk of miscalculation—for instance, a third-party cyber intrusion being misinterpreted as an attempt by one side to target the other's NC3.

Several options could be pursued to operationalize such a commitment. Which options would be most desirable and feasible, however, depend in part on how willing each side is to disclose what it considers to be its core NC3 architecture. These options are listed in order of descending ambition and difficulty of implementation.

1. Both sides could agree on a *generic* description of core NC3 components that would then be off limits for cyber intrusions. This could include one or more of the following elements: command and control posts; early-warning systems (including satellites and radar); nuclear weapons and delivery systems; the connections between each of these elements and between them and national leadership; and essential support infrastructure (like power supplies) for each element.

2. Each side could elect to designate some elements of its core NC3 systems as off limits, and then share that list with the other side. The notification could be reciprocal, but it need not be conditioned on reciprocity (full or otherwise). If one side were to accept this commitment but choose not to communicate which elements they consider part of their core NC3, it would have to accept that the other side might intrude inadvertently into those systems without violating the commitment.

3. Both sides could agree to exercise extreme caution to avoid targeting the other's core NC3 systems, without attempting to share precisely what those elements are. However, if one side detects a cyber intrusion—attributed to the other—into some element its NC3 system that it believes to play a core role, the target would notify the suspected intruder that it appears to have

trespassed into core NC3. The intruder would then be expected to cease and withdraw immediately, unless it is able to explain its conduct in a way the other side deems reassuring. If the suspected party were not responsible for the intrusion, it could help identify the intruder.

4. One or more of the above commitments could be made to apply solely under peacetime conditions. The United States and/or China could indicate, explicitly or implicitly, that if actual fighting were to take place, all prior commitments would be suspended.

Chinese participants generally perceived the United States as able and willing to conduct cyber operations to penetrate and attack China's dual-use conventional NC3 systems. Both long-existing and recently adopted policies show that the United States would be inclined to do so if war broke out. Thus, Chinese experts generally would welcome measures of self-restraint like those described above, believing they would reduce pressures on China to increase and diversify its nuclear arsenal and raise the alert levels of its nuclear forces. Chinese participants also suggested that China would not be inclined to conduct cyber operations against U.S. NC3, because they doubt that China is presently capable of launching a similarly effective attack.

For all the reasons that Chinese experts would welcome such restraints, U.S. experts find them either inadvisable or impractical. Their main concern is that restraints of this type could weaken U.S. deterrence. Because these experts assume that China would be the instigator of conflict, they are reluctant to eschew cyber capabilities and planning to reduce China's capabilities to escalate conflict through use of conventional and/or nuclear missiles. This reinforces the Chinese perception that U.S. cyber operations against their command and control systems could be less detectable and more widely effective than conventional or nuclear strikes alone. Further complicating the issue, U.S. experts doubt that China would make and uphold similar commitments even if the United States were to commit to such restraints.

In general, it would be extremely difficult for either side to persuade the other of its adherence to restraint—or to verify that the other side is doing the same. Thus, American experts generally profess considerable skepticism over the viability of this approach. This does not entirely negate its value in stimulating thinking and periodically revisiting the analysis of the trade-offs associated with these or similar options.

U.S. experts suggest more modest steps that each country could take to ameliorate risk. The United States, they propose, should involve cyber-nuclear force operators and policymakers in thoughtful classified assessments of any risks that cyber operations against Chinese NC3 systems could create or intensify. Such studies should address possible unintended consequences of malware propagating into systems beyond those that are the intended target, and other steps that could be misinterpreted

by their Chinese counterparts. Further, U.S. cyber-nuclear operators and policymakers should conduct tabletop exercises to explore and better understand such dynamics, and how to avoid those that would be especially likely and/or dangerous. While Chinese cyber-nuclear operators and policymakers may start from different assumptions than their U.S. counterparts, there is reason to believe that they too would gain from conducting similar internal analyses and exercises regarding unintended consequences of cyber espionage and potential attacks on U.S. NC3. Such steps would help prepare them to identify and enact unilateral restraint measures with which they would be comfortable, and to engage in bilateral dialogue on these issues.

Meanwhile, as an interim measure, relevant U.S. and Chinese experts and officials could consider whether they would find it helpful and feasible for both countries to declare that they would view any attempt by the other to interfere with the effective operations of NC3 as a grave threat to security. Further, they could acknowledge their understanding that the other would view such an attempt similarly. This understanding could be conveyed privately by officials at the highest levels. This would convey the added value that multiple agencies involved in these issues have educated their senior leaders about their importance.

Commitment to high-level authorization for cyber operations targeting NC3

Drawing from the discussion above, another way to improve stability would be for the United States and China to declare that, in a conflict, any decision to intentionally *attack* nuclear weapons and NC3 systems—by any means, including cyber operations—should be made by the highest-level authority as would authorize nuclear use. Though the decision to attack nuclear weapons and NC3 systems has always been reserved for the highest-level authority, it is not clear whether actions taken via cyber means are included. Considering how cyber operations can incur unintended effects, such a commitment could be meaningful for both sides to lessen suspicions and build confidence. A related way to make or affirm this understanding would be to clarify that senior leaders (up to the presidential level) would be considered accountable for any actions along these lines taken by cyber operators under their control, even if not expressly authorized.

Commitment not to target space-based strategic assets

The use of cyber means in space and anti-space warfare poses an extremely dangerous and complex challenge. The United States explicitly seeks to maintain "space superiority" over Russia, China, and everyone else.[49] Russia and China seek to prevent this. Because NC3 systems depend in many ways on space-based assets, there is a significant risk that space and counterspace warfare could damage these systems (particularly functions related to navigation, early warning, and communications). To the extent that cyber capabilities could be used as part of space warfare, this dynamic is part of the cyber-nuclear challenge.

Therefore, it is worth exploring whether the United States and China could agree on some norms pertaining to space and anti-space warfare that would preclude some or all attacks on space-based strategic/early-warning assets. This could apply solely to cyber means or preclude all means of targeting such assets. It could apply to specific kinds of attacks (for example, by banning spoofing but allowing for jamming) to minimize the risk of triggering false alarms or panic over the inability to produce a solid situational awareness. While such a commitment would be more limited in scope than excluding attacks on all NC3, it may be more expedient. For example, it would not require either side to delineate the boundaries of NC3 or explicate the purpose of systems that may be single or dual use. Moreover, precluding all forms of attack would avoid the ambiguity over what constitutes legitimate attack vectors or tools.

Commitment to restrain third-party cyber activities

Participants from both countries fully agreed that the third-party factor is extremely destabilizing to the cyber-nuclear nexus. There are at least six possibilities (three forms of apparent third-party action, each of which could go two ways): A third party could disguise itself as either China or the United States while launching operations against the other. China or the United States could disguise themselves as a third party when attacking the other (known as a false-flag operation). Or China or the United States could activate proxies to conduct cyber operations against the other.

Similar opportunities for third parties to manipulate crises and conflicts simply do not exist in the kinetic world. The United States and China should agree to exercise effective oversight and control over destabilizing cyber activities of third parties that have one or more of the following characteristics:

1. under their direction;

2. using their territory to conduct operations;

3. employing capabilities that they have developed; or

4. allies over whom they wield considerable influence and whose actions could trigger or escalate crises involving both the United States and China.

In our discussions, U.S. experts emphasized the shared interest in taking steps to mitigate third-party risks, and believe that the United States would regard such steps by China as a meaningful gesture that would help build trust. Chinese experts doubted that such commitments are feasible in the current political environment. Nevertheless, it is worthwhile to keep this option in mind for when the political environment would facilitate such understandings.

Dialogue and Information Sharing

Clearly, the lack of meaningful dialogue about—let alone mutual understanding of—responsible conduct in cyberspace hinders both countries from mitigating these risks. Again, this problem is especially acute regarding the ultra-secretive and ultra-sensitive nexus between cyber and nuclear operations.

In the U.S.-Russia experience, dialogues on strategic stability helped create a shared basis for each side to calibrate its own actions and interpret messages sent by the other during crises. The absence of such a foundation between the United States and China amid escalating risks of confrontation and miscalculation is acutely concerning.

One reason why Washington resists acknowledging mutual vulnerability with China as a basis of strategic stability is that the United States provides extended nuclear deterrence to protect the security of its allies in Asia (and the North Atlantic Treaty Organization). These allies worry that the United States will be less likely to defend them in a conflict with China if China threatens the existence of the United States with nuclear weapons. These allies and the United States are increasingly concerned about the rapid development of China's conventional capabilities to project its own power, and its increasingly visible efforts to assert its military presence in Asia, undercut U.S. extended security guarantees to its regional allies, and deny U.S. military forces access to and freedom of operation in this area.

Though Washington would clearly prefer to not use nuclear weapons, it must consider this possibility in the event of conflict involving China and U.S. allies. If necessary, the United States probably would initially use cyber and conventional capabilities to preemptively attack China's nuclear retaliatory forces. But it could possibly employ nuclear strikes as well in the most extreme circumstances.[50] Such "damage-limiting" attacks on China's nuclear capabilities would be meant to provide time and space for U.S. and allied conventional forces to roll back assumed Chinese gains in the earlier stages of the imagined conflict.[51]

China may believe commitments such as its no-first-use policy reassure its neighbors and the United States. Indeed, China insists that it maintains a much more recessed nuclear launch doctrine than that of the United States.[52] The relatively small size of China's nuclear arsenal is consistent with this doctrine and would not make a damage-limiting (or first-strike) strategy feasible against the United States or Russia. Instead, China seeks capabilities to ensure its nuclear deterrent can survive against potential U.S. attacks and to retain the deterring capacity to inflict massive retaliatory damage.

However, U.S. experts view commitments like no first use as questionable and unverifiable, and they place far greater value on frank dialogue. They also doubt whether such a policy reflects China's actual intentions or likely behavior in a conflict.

U.S. observers find it very difficult to redress Chinese concerns over strategic stability arising from the U.S. nuclear posture. For example, Washington officially articulated in the 2019 Missile Defense Review that its missile defenses would not be aimed at negating the core nuclear forces of either Russia or China.[53] Yet, most Chinese experts do not find such inferences especially reassuring. The United States' ongoing efforts to augment its capacity to launch first strikes with its conventional and nuclear forces—along with ballistic missile defenses and perhaps cyber operations—make Chinese observers doubt Washington's professed defensive intentions. Chinese (and other) observers also note that U.S. rhetoric and policies change frequently with new administrations, which makes it difficult to understand U.S. intentions and trust its reassurances. Prudent planners naturally then feel that they must assume the worst about U.S. capabilities—both those that exist and those that are being sought. Even if the United States were to accept mutually assured destruction (MAD) as a basis for strategic stability with China, it might hardly reassure Beijing. Chinese observers emphasize that "MAD itself [is] an aggressive way of thinking" that does not "accord with China's nuclear policy," which is defensive and keeps "its nuclear capabilities at the minimum level required for national security."[54]

In the cyber domain, China stresses that an overemphasis on cybersecurity, especially in the military and spheres, will hamper the application of ICT in social and economic development. China rallies others not "to give up on efforts" to "de-militarize and de-weaponize cyberspace."[55] In the words of Xu Peixi, a Chinese analyst, "we make rules exactly because we want the cyberspace to no longer be a battlefield."[56] Some established Chinese experts hold negative attitudes toward the discussion of military doctrines governing cyber operations. They point out technical difficulties in applying the law of armed conflict to cyberspace. The most fundamental starting point, in their opinion, is to achieve consensus on core issues such as cyber sovereignty. Otherwise, discussions of cyber military transparency and doctrines will be meaningless in maintaining cyber stability between the two countries. They also recall favorably when Obama said in September 2015 that while the United States is prepared to win if cyber becomes an area of competition, the United States prefers to establish basic rules of the road to avert cyber conflict.[57] Certainly, these Chinese experts would prefer that the United States concentrate on building norms against offensive cyber operations.

Leading U.S. experts, on the other hand, believe that China's stated preference for an exclusively peaceful and cooperative cyberspace is naïve, duplicitous, or both. They suggest that the chances of stability would improve if China would join the United States in acknowledging their military cyber

capabilities and explaining their purposes and doctrines. It could provide the basis for meaningful dialogues on principles of responsibility and accountability to manage what Joseph Nye Jr. has called their "cooperative rivalry," and then on how to deal with potential cyber operations against capabilities that could affect NC3. U.S. participants in this project acknowledged that the United States can and should do more to clarify its own policies in this area and strive for more coherent and consistent communications of them.

We consider it essential that the United States and China find ways to talk with each other in an appropriate official setting covering three main topics. They could start by developing a mutual understanding of steps that one or both states find destabilizing and those that both agree are stabilizing. For example, to ease Chinese concerns, the United States could clarify that it acknowledges it cannot successfully escape from being vulnerable to Chinese nuclear retaliation, and then look for concrete ways to reassure China that it indeed plans to behave accordingly. The United States' willingness to limit its military competition with China, in turn, will depend heavily on China demonstrating its understanding that strategic stability requires not using force or physical actions to change the territorial status quo and assert unilateral definitions of land, sea, or air boundaries.

To reduce anxieties and instabilities that may be caused by cyber threats to NC3 systems, the two sides will also need to have expert-level talks to discuss relevant issues more broadly. Among them, they would probably wish to address their concerns about the vulnerability of NC3 systems and explore how the integration of command and control for conventionally armed delivery systems and nuclear weapons may increase risks of inadvertent escalation, especially from cyber attacks. Another topic that experts would be expected to address is how blurring the lines between nuclear and conventional assets and introducing certain types of missile defense could upset the strategic balance.[58] Both sides presumably also would wish to discuss perceived changes in each other's nuclear postures and deployments and testing programs.[59]

Beyond airing concerns, such conversations could explore whether there are steps the parties could take together to reduce these risks. Possible steps could range from policy declarations to confidence-building measures regarding exercises and deployments to, eventually, limits on the number of various offensive and, perhaps, defensive systems.

Another potential area for discussion is China's general lack of transparency around its nuclear arsenal and modernization efforts, which is one of the United States' chief concerns. China may be reluctant to engage in dialogue on these issues due to the traditional view that ambiguity can help offset U.S. advantages. Yet, some participants acknowledged an alternative perspective: low transparency by the less capable side could embolden the party with superior capability to overreact in a

conflict. For its part, China could seek more transparency regarding U.S. ballistic missile defense plans and capabilities. In our view, the divergent views on these issues could themselves be useful topics for China-U.S. dialogue on the cyber-nuclear nexus.

A second basket of topics to cover in the dialogue would be the potential benefits and risks of offensive cyber operations, especially as they pertain to the cyber-nuclear nexus. Such dialogue ought to be carried out as a matter of strategic analysis rather than a forum for exchange of political accusations. Insofar as China has publicly acknowledged that it has military cyber capability (which could inherently be used to conduct attacks), we do not believe that it is wise to set preconditions for such an exchange. A dialogue could make it easier to clarify to each other the types of restraint that would be most important for strategic stability. It could cover how each side views cyber operations, including what would be seen as escalatory and how each might try to signal willingness to de-escalate or pursue off-ramps. This could help prevent inadvertent escalation in crises or conflict.

Most immediately, China could shed some light in a proper bilateral setting on the nature of its internal processes and oversight of cyber and other relevant capabilities. The United States, of course, would be expected to reciprocate in a forthcoming manner. China also could address destabilizing activities (for example, the use of blinding lasers) that fuel broader concerns over its intentions and organization.

The United States and China could also, in principle, pursue an understanding, perhaps even explicit agreements, on some types of information sharing that would apply in peacetime. For example, they could share cyber threat intelligence of common interest. Admittedly, such information sharing would not have an immediate bearing on the cyber-nuclear nexus, nor would it necessarily apply in times of outright confrontation. Nevertheless, the existence of a process to establish and foster effective implementation of such norms could help usher in a more constructive atmosphere for handling bilateral cyber-nuclear challenges. Such a bilateral communications channel should ideally also include an option for exchanging messages of alarm and reassurance on an ad hoc basis (such as during a crisis).

While participants from both countries agreed in principle on the potential value of such information sharing, they were not clear on what types of information could be exchanged. They also doubted its feasibility in the current political environment. That said, they agreed that the current channel between CERTs from both sides could be broadened to share more threat information that could have strategic consequences. Another option is to functionalize part of the current U.S.-China Law Enforcement and Cybersecurity Dialogue within the framework of the U.S.-China Comprehensive Dialogue into a real-time response mechanism. Notwithstanding the difficulties inherent in institutionalizing broad bilateral cyber-specific information exchange and agreeing on common norms of

restraint—as well as the long-lasting differences on how to build mutual trust as discussed earlier—all participants in this project concurred that China and the United States should quickly establish a dialogue on cyber risks to NC3 systems. Some of it can overlap with the dialogues we proposed earlier so the two sides can communicate their respective perceptions and concerns about cyber threats, cyber stability, and cyber strategies and policies in general. But some dialogue should focus on risks and remedies specific to NC3. Both sides could convey policies and practices they have put in place to prevent inadvertent escalation to nuclear war, which would then open the way for addressing each other's concerns.

U.S. participants in this project, from diverse political and strategic perspectives, uniformly concluded that such dialogue would be timely, necessary, and invaluable for reducing the risks this paper has explored, as well as paving the way for China-U.S. crisis management. They also suggested that this unclassified paper could form the basis for discussion of issues that might now be too sensitive for either government to articulate. Chinese participants also largely concurred with this recommendation, even as they noted reservations that the United States is the stronger party and, in their view, may derive a greater advantage from dialogue on these issues. U.S. experts acknowledged this concern, even as they viewed it to be unfounded. One value of this paper, then, could be to identify issues that officials from both governments could address without having to present them as official positions or concerns.

If China and the United States conclude that dialogue is necessary and practical, an early step would be to consider which fora would be most conducive for conducting such a dialogue. Existing communication channels might be suitable for some types of information exchange. New ones could be created to address other issues. The following forums could be considered:

- The existing Diplomatic and Security Dialogue can be a channel for high-level officials on either side to express concerns over the other's policy changes and share major developments in their own capabilities or policies.

- Two MOUs signed in 2014 between the U.S. Department of Defense and the Chinese Ministry of National Defense offer potential venues for military-to-military dialogue: the MOU on Notification of Major Military Activities and the MOU on Rules of Behavior for the Safety of Air and Maritime Encounters. The two militaries could discuss extending the latter MOU to discuss basic principles of conduct for cyber operations.

- Another potential mechanism is the U.S.-China Joint Staff Dialogue between both sides' J5 directorate (which oversees strategy, policy, and planning), which was established in 2017 but suspended in 2018. Crisis management was the main topic of the first meeting. Once resumed, it

could be used as the platform for more detailed discussions of capabilities and intentions of cyber forces and concerns about perceived cyber threats to NC3 systems between mid-level officials.

- For communication during a major cyber incident or crisis, established channels between designated higher-level officials would be most useful to prevent misunderstanding, coordinate emergency responses, or notify the other side of possible responses to major cyber attacks.

- The existing coordination mechanism between both countries' CERTs could continue to serve as the primary channel for general cooperation and could be broadened to cover information on threats with potential strategic consequences.

- For crisis communications, the existing hotline between the Chinese Ministry of National Defense and the U.S. Department of Defense can be utilized. It seems to be well suited for communication on cyber issues pertaining to NC3.

One question to consider is how to make sure diplomatic coordination can be involved in the process whenever appropriate. One option is to refer to a pre-designated diplomatic channel communication related to attribution in the event of a suspected attack or third-party interference, including to clarify that the United States/China is not involved in a suspected cyber operation.

Concluding Thoughts

This paper emerged from extensive dialogues between U.S. and Chinese experts on strategic affairs who convened over several years to discuss dynamics they felt could take both countries in highly undesirable directions. They were initially uncertain whether such a delicate and sensitive topic could be meaningfully discussed in a nongovernment settling, let alone bilaterally. Thus, they cautiously explored whether the necessary knowledge base and interest existed in both governments to support an unofficial, expert-level study group such as this. Once they were reassured that the respective governments would welcome such a research project (without any prior commitment to endorse its findings), the experts came together to work out the terms of reference for the project, to define its scope, and to agree on the modalities for pursuing it.

Over time, it has become clear to the participants that the cyber-NC3 nexus within and between both countries indeed presents daunting and potentially ominous challenges. We have endeavored to describe and explain these challenges throughout this paper. The lengthy discussion of challenges reflects the participants' assessment of the gravity of the dangers posed by cyber threats to NC3, as well as their sense that these dangers are not (yet) widely understood. These challenges arise at the

intersection of two highly specialized, secretive, and tightly compartmented domains that constantly evolve. The personnel in these two domains rarely engage in serious systematic exchanges. Moreover, the competitive, partially conflictual context in which U.S. and Chinese cyber-nuclear operators and policymakers prepare to operate against each other (if called to do so) intensifies the challenge of developing mutual understanding among and between them. Our hope is that the first part of the paper demonstrated the urgent need for each of the countries to look closely and holistically at the cyber-NC3 nexus. It also aims to provide a common analytic basis for them to do so in ways that do not compromise secrecy or overly encroach on compartmentation.

The second part of the paper discussed ways in which China and the United States might begin to address these risks and challenges individually and hopefully also cooperatively. The experts have noted why some of the remedies discussed herein would be (at least initially) far tougher to pursue bilaterally. This stems naturally from a combination of profound distrust of the other's intentions, deeply rooted proclivities to address security challenges in certain ways, and structural asymmetries between the United States and China in the cyber and nuclear domains. The United States' competition with Russia also complicates China's perceptions of U.S. threats, and limits Washington's capacity to reassure China. Nevertheless, participants concluded that there are ways to make meaningful cooperative progress in addressing the risks inherent in the intersection between nuclear and cyber weapons, especially those related to the extremely sensitive NC3 systems of both parties.

Participants concluded this study convinced that China and the United States share enough common interest in avoiding an armed conflict and escalation toward nuclear exchanges that the two countries could find it possible to work toward the shared goal of diminishing cyber threats to NC3. They believe that the most feasible way to proceed is for both parties first to engage in internal reviews and brainstorming, red teaming, and table-top exercises that could then inform briefings to the top leadership in each country. This process could itself yield immediate dividends by easing some friction between the United States and China on strategic matters in general and NC3 in particular.

Subsequently the parties could then be ready to proceed cautiously to initiate bilateral dialogue between specially designated interlocutors on both sides. Such dialogue could build on one or more of the existing institutionalized channels for bilateral dialogue. The aim would be to help both parties better appreciate their respective concerns, concepts, and policies, and address at least some of these concerns constructively. If initial bilateral dialogues prove beneficial and the broader political relationship between China and the United States improves, the two sides could design and agree upon measures to restrain themselves and each other from taking actions that would be most destabilizing in the cyber-nuclear nexus.

Notes

1 Joe Biden, "A Letter to Dr. Eric S. Lander, the President's Science Advisor and nominee as Director of the Office of Science and Technology Policy," White House official website, published January 20, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/01/20/a-letter-to-dr-eric-s-lander-the-presidents-science-advisor-and-nominee-as-director-of-the-office-of-science-and-technology-policy/.

2 Xi Jinping, "Remarks by H.E. Xi Jinping President of the People's Republic of China At the Opening Ceremony of the Second World Internet Conference," Ministry of Foreign Affairs of the People's Republic of China, December 16, 2015, https://www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t1327570.shtml.

3 For the purposes of our discussions, we define nuclear command, control, and communications (NC3) as the entire apparatus of information and telecommunication facilitating and supporting the operations of nuclear forces and assisting nuclear weapons decisionmaking. Importantly, NC3 also includes auxiliary systems (such as power supplies) that are vital to their functioning and potentially vulnerable to cyber attack. Nuclear-armed states require NC3 to function from early warning all the way to the conduct of nuclear operations.

4 The most obvious risks are between the United States and Russia, the United States and China, and India and Pakistan.

5 Jason Fritz, "Hacking Nuclear Command and Control," International Commission on Nuclear Non-proliferation and Disarmament, 2009, http://www.icnnd.org/Documents/Jason_Fritz_Hacking_NC2.pdf.

6 Defense Science Board, "Task Force Report: Resilient Military Systems and the Advanced Cyber Threats," U.S. Department of Defense, 2013, https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-081.pdf.

7 Robert Burns, "Ex-commander: Nukes on High Alert Are Vulnerable to Error," Associated Press, April 30, 2015, https://apnews.com/e970363945364db79dff94240956e2c4.

8 Nicholas Watt, "Trident Could Be Vulnerable to Cyberattack, Former Defence Secretary Says," Guardian, November 23, 2015, https://www.theguardian.com/uk-news/2015/nov/24/trident-could-be-vulnerable-to-cyber-attack-former-defence-secretary-says.

9 M.V. Ramana and Mariia Kurando, "Cyberattacks on Russia—the Nation with the Most Nuclear Weapons—Pose a Global Threat," Bulletin of the Atomic Scientists 75, no. 1 (2019): 44–50.

10 "Statement for Cooperation among Governments to Address Cyber Threats to Nuclear Weapon Systems," Euro-Atlantic Security Leadership Group, February 2019, https://www.europeanleadershipnetwork.org/wp-content/uploads/2019/02/EASLG-Statement_Cyber-Threats_FINAL.pdf. The statement added: "Cyber threats to nuclear weapons systems increase the risk of use as a result of false warnings or miscalculation, increase the risk of unauthorized use of a nuclear weapon, and could undermine confidence in the nuclear deterrent, affecting strategic stability."

11 Theresa Hitchens, "HASC Adds NC3 Funds; Wants Talks with Russia, China," Breaking Defense, June 10, 2019, https://breakingdefense.com/2019/06/hasc-adds-nc3-funds-wants-talks-with-russia-china/.

12 Page O. Stoutland and Samantha Pitts-Kiefer, "Nuclear Weapons in the New Cyber Age," Nuclear Threat Initiative, September 2018, https://media.nti.org/documents/Cyber_report_finalsmall.pdf; Beyza Unal and Patricia Lewis, "Cybersecurity of Nuclear Weapon Systems: Threats, Vulnerabilities and Consequences," Chatham House, January 2018, https://www.chathamhouse.org/sites/default/files/publications/research/2018-01-11-cybersecurity-nuclear-weapons-unal-lewis-final.pdf.

13 Andrew Futter, Hacking the Bomb: Cyber Threats and Nuclear Weapons (Washington, DC: Georgetown University Press, 2018), 124.

14 David C. Gompert and Martin Libicki, "Cyber War and Nuclear Peace," Survival 61, no. 4 (2019): 45–62.

15 Jon R. Lindsay, "Cyber Operations and Nuclear Weapons," Nautilus Institute, June 20, 2019, https://nautilus.org/napsnet/napsnet-special-reports/cyber-operations-and-nuclear-weapons/.

16 See, for instance, James M. Acton, "Escalation Through Entanglement: How the Vulnerability of Command-and-Control Systems Raises the Risks of an Inadvertent Nuclear War," International Security 43, no. 1 (Summer 2018); Erik Gartzke and Jon R. Lindsay, "The Cyber Commitment Problem and the Destabilization of Nuclear Deterrence," in Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations, eds. Herbert Lin and Amy Zegart (Washington, DC: Brookings Institution Press, 2018); Lawrence J. Cavaiola, David C. Gompert, and Martin Libicki, "Cyber House Rules: On War, Retaliation and Escalation," Survival 57, no. 1 (2015): 81–104; Paul Bracken "The Cyber Threat to Nuclear Stability," Orbis 60, no. 2 (2016); Stephen J. Cimbala and Roger N. McDermott, "A New Cold War? Missile Defenses, Nuclear Arms Reductions, and Cyber War," Comparative Strategy 34, no. 1 (2015): 95–111.

17 See, for instance, Mark Fitzpatrick, "Artificial Intelligence and Nuclear Command and Control," Survival 61, no. 3 (2019).

18 See, for instance, Xu Longdi, "Cyberattack, Nuclear Safety and Strategic Stability," in Information Security and Communications Privacy 9 (2018); Xu Weidi, "Strategic Stability and its Relations with Nuclear, Outer Space and Cyberspace," Information Security and Communications Privacy 9 (2018); Cui Jianshu, "Modernization of Nuclear Power of the US and Strategic Stability in Cyberspace," China's Information Security 8 (2019); Jiang Tianjiao, "Cross Domain Deterrence and Strategic Stability in Cyberspace," China's Information Security 8 (2019).

19 According to a joint advisory by the U.S. National Security Agency (NSA) and UK National Cyber Security Centre (NCSC), the Russian hacker group "accessed and used the Command and Control (C2) infrastructure of Iranian APTs to deploy their own tools to victims of interest." This series of operations occurred over the course of several years. See NCSC and NSA, "Advisory: Turla Group Exploits Iranian APT to Expand Coverage of Victims," NCSC, October 21, 2019, https://www.ncsc.gov.uk/news/turla-group-exploits-iran-apt-to-expand-coverage-of-victims; Jack Stubbs and Christopher Bing, "Hacking the Hackers: Russian Group Hijacked Iranian Spying Operation, Officials Say," Reuters, October 21, 2019, https://www.reuters.com/article/us-russia-cyber/hacking-the-hackers-russian-group-hijacked-iranian-spying-operation-officials-say-idUSKBN1X00AK.

20 Andy Greenberg, "The Untold Story of the 2018 Olympics Cyberattack, the Most Deceptive Hack in History," Wired, October 17, 2019, https://www.wired.com/story/untold-story-2018-olympics-destroyer-cyberattack/.

21 Caitlin Talmadge, "The US-China Nuclear Relationship: Why Competition Is Likely to Intensify," Brookings Institution, September 2019, https://www.brookings.edu/wp-content/uploads/2019/09/FP_20190930_china_nuclear_weapons_talmadge-2.pdf, 3.

22 Office of the Secretary of Defense, "Summary of the 2018 National Defense Strategy of the United States of America," U.S. Department of Defense, 2018, https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

23 Adam P. Liff and G. John Ikenberry, "Racing Toward Tragedy? China's Rise, Military Competition in the Asia Pacific, and the Security Dilemma," International Security 39, no. 2 (Fall 2014): 52–91.

24 The APT1 report, published in 2013 by U.S. cybersecurity company Mandiant, accused the Chinese military of a massive cyber espionage campaign beginning in 2006, targeting 141 organizations in the

United States and elsewhere. See "APT1: Exposing One of China's Cyber Espionage Units," FireEye Mandiant, February 18, 2013, https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf.

25 On June 4, 2015, the Office of Personnel Management (OPM) announced that over four million federal employees' personally identifying information was compromised by a cyber data breach. It is widely reported that the cyber attack was carried out by state-sponsored attackers for the Chinese government. See, for example: Josh Fruhlinger, "The OPM Hack Explained: Bad Security Practices Meet China's Captain America," CSO, February 12, 2020, https://www.csoonline.com/article/3318238/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html; Ellen Nakashima, "Chinese breach data of 4 million federal workers," Washington Post, June 4, 2015, https://www.washingtonpost.com/world/national-security/chinese-hackers-breach-federal-governments-personnel-office/2015/06/04/889c0e52-0af7-11e5-95fd-d580f1c5d44e_story.html.

26 Details of bilateral dialogues on cyber security can be found at: Lu Chuanying, "China-US Cyberspace Relations in the Trump Era," China-US Focus, December 29, 2017, https://www.chinausfocus.com/peace-security/china-us-cyberspace-relations-in-the-trump-era.

27 "China's National Defense in the New Era," Chinese Ministry of National Defense, 2019, p. 9, http://eng.mod.gov.cn/news/2019-07/24/content_4846443.htm.

28 See "Achieve and Maintain Cyberspace Superiority: Command Vision for U.S. Cyber Command," U.S. Cyber Command, March 23, 2018, https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010; Paul M. Nakasone, "A Cyber Force for Persistent Operations," Joint Force Quarterly 92 (2019): https://www.459arw.afrc.af.mil/News/Article-Display/Article/1737519/a-cyber-force-for-persistent-operations/.

29 "Summary: Department of Defense Cyber Strategy 2018," U.S. Department of Defense, 2018, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

30 Ellen Nakashima, "White House Authorizes 'Offensive Cyber Operations' to Deter Foreign Adversaries," Washington Post, September 20, 2018, 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.

31 "An Interview with Paul M. Nakasone," Joint Forces Quarterly 92, no. 1 (2019): https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92.pdf.

32 [30] Paul M. Nakasone and Michael Sulmeyer, "How to Compete in Cyberspace," Foreign Affairs, August 25, 2020, https://www.foreignaffairs.com/articles/united-states/2020-08-25/cybersecurity.

33 Nele Achten, "New U.N. Debate on Cybersecurity in the Context of International Security," Lawfare, September 30, 2019; https://www.lawfareblog.com/new-un-debate-cybersecurity-context-international-security.

34 "Communication from the United States: Measures Adopted and Under Development by China Relating to its Cybersecurity Law," World Trade Organization, September 26, 2017, https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/S/C/W374.pdf.

35 "APT1: Exposing One of China's Cyber Espionage Units," FireEye Mandiant.

36 Bojan Pancevski, "U.S. Officials Say Huawei Can Covertly Access Telecom Networks," Wall Street Journal, February 12, 2020, https://www.wsj.com/articles/u-s-officials-say-huawei-can-covertly-access-telecom-networks-11581452256.

37 "Foreign Ministry Spokesperson Zhao Lijian's Regular Press Conference on October 21, 2020," Chinese Ministry of Foreign Affairs, October 21, 2020, https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/t1825675.shtml.

38 "Foreign Ministry Spokesperson Zhao Lijian's Regular Press Conference on August 18, 2020," Chinese Ministry of Foreign Affairs, August 18, 2020, https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/t1807193.shtml; "Foreign Ministry Spokesperson Hua Chunying's Regular Press Conference on December 10, 2020," Chinese Ministry of Foreign Affairs, December 10, 2020, https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/t1839270.shtml.

39 Lu Chuanying, "China-US Cyberspace Relations in the Trump Era."

40 Ibid.

41 Acton, "Escalation Through Entanglement."

42 Colin Clark, "Nuclear C3 Goes All Domain: Gen. Hyten," Breaking Defense, February 20, 2020, https://breakingdefense.com/2020/02/nuclear-c3-goes-all-domain-gen-hyten/.

43 In the context of cyberspace, the key metrics for assessing the sophistication of an offensive operation are its confidentiality, plausible deniability, precision, assured effects, timeliness, and avoidance of collateral damage.

44 See also John R. Harvey, "U.S. Nuclear Command and Control for the 21st Century," Nautilus Institute, May 24, 2019, https://nautilus.org/napsnet/napsnet-special-reports/u-s-nuclear-command-and-control-for-the-21st-century/.

45 The three factors mentioned here, including third-party actors in cyberspace, attribution challenges, and attackers' and targets' abilities to assess the effects of an operation, have been elaborated in other parts in this paper. The third-party factor was explained in the "Introduction," while explanations of the other two can be seen in the section on "Cyber-Nuclear Risks: Scenarios of Particular Concern."

46 Office of the Secretary of Defense, "2018 Nuclear Posture Review," U.S. Department of Defense, February 2018, https://media.defense.gov/2018/Feb/02/2001872886/-1/-1/1/2018-NUCLEAR-POSTURE-REVIEW-FINAL-REPORT.PDF.

47 Peter Feaver and Kenneth Geers, "'When the Urgency of Time and Circumstances Clearly Does Not Permit…': Pre-delegation in Nuclear and Cyber Scenarios," in Understanding Cyber Conflict: 14 Analogies, eds. George Perkovich and Ariel E. Levite (Washington, D.C.: Georgetown University Press, 2017).

48 David Hoffman, The Dead Hand: The Untold Story of the Cold War Arms Race and Its Dangerous Legacy (New York: Random House, 2014).

49 United States Space Command, "Vision for 2020," The Community, August 26, 2018, https://thecommunity.com/vision-for-2020; "Remarks by President Trump at a Meeting with the National Space Council and Signing of Space Policy Directive-3," Executive Office of the President, June 18, 2018, https://www.whitehouse.gov/briefings-statements/remarks-president-trump-meeting-national-space-council-signing-space-policy-directive-3/.

50 The paper newly produced by the U.S. State Department describes why and how the 2018 Nuclear Posture Review clarified "'the extreme circumstances' under which the United States does not a priori rule out the possibility of using nuclear weapons," and adds further that "deterring limited nuclear attacks on allies and deployed U.S. forces" is the most urgent nuclear deterrence challenge today. See: Office of the Under Secretary of State for Arms Control and International Security, "Strengthening Deterrence and Reducing Nuclear Risks: The Supplemental Low-Yield U.S. Submarine-Launched Warhead," U.S. State Department, April 24, 2020, https://www.state.gov/wp-content/uploads/2020/04/T-Paper-Series-4-W76.pdf.

51 Elbridge Colby, "The Need for Limited Nuclear Options," in Challenges in U.S. National Security Policy: A Festschrift Honoring Edward L. (Ted) Warner, eds. David Ochmanek and Michael Sulmeyer (Santa Monica, CA: RAND Corporation, 2014), https://s3.amazonaws.com/files.cnas.org/documents/The-Need-for-Limited-Nuclear-Options-Colby-Chapter1.pdf.

52 See, for instance, Li Bin and Tong Zhao, eds., "Understanding Chinese Nuclear Thinking," Carnegie Endowment for International Peace, 2016, https://carnegieendowment.org/files/ChineseNuclearThinking_Final.pdf.

53 In the 2019 Missile Defense Review, the U.S. Department of Defense declared that "U.S. missile defense capabilities will be sized to provide continuing effective protection of the U.S. homeland against rogue states' offensive missile threats. The United States relies on nuclear deterrence to address the large and more sophisticated Russian and Chinese intercontinental ballistic missile capabilities." See: Office of the Secretary of Defense, "2019 Missile Defense Review," U.S. Department of Defense, 2019, https://www.defense.gov/Portals/1/Interactive/2018/11-2019-Missile-Defense-Review/The%202019%20MDR_Executive%20Summary.pdf.

54 "China's National Defense in the New Era," Chinese Ministry of National Defense.

55 Xu Peixi, "Nine Areas of Disputes in the Debate on International Cyber Norms," China Institute for International Strategic Studies, https://ceipfiles.s3.amazonaws.com/pdf/CIISS_Nine+Areas+of+Dispute+in+the+Debate+on+International+Cyber+Norms+-+full.pdf.

56 Ibid.

57 Office of the Press Secretary, "Remarks by the President in Town Hall at Fort Meade," White House, September 11, 2015, https://obamawhitehouse.archives.gov/the-press-office/2015/09/14/remarks-president-town-hall-fort-meade.

58 James M. Acton, "Is It a Nuke?: Pre-Launch Ambiguity and Inadvertent Escalation," Carnegie Endowment for International Peace, 2020, https://carnegieendowment.org/2020/04/09/is-it-nuke-pre-launch-ambiguity-and-inadvertent-escalation-pub-81446.

59 Given China's reliance on a limited nuclear arsenal, the possibility of the United States developing and deploying missile defense systems that could reliably be effective against China's nuclear-armed missiles raises further alarm in Beijing. However, the missile defenses tested and deployed by the United States would not be reliably effective to date against the Chinese nuclear arsenal. Unlike the United States, China reportedly does not in peacetime keep its land- and air-based nuclear forces on alert and ready to be launched within minutes. The operational strategy of China's sea-based nuclear forces is unknown. However, as China starts to deploy its strategic nuclear submarines on deterrent patrols, it may face a greater pressure to deploy nuclear warheads on patrolling submarines. This would at least technically shorten the time between decisions to launch nuclear weapons and their actual launch. It could also introduce a measure of complexity into the preexisting NC3 architecture. More details can be seen at: Tong Zhao, "Managing the Sino-American Dispute over Missile Defense," War on the Rocks, August 11, 2020, https://warontherocks.com/2020/08/managing-the-sino-american-dispute-over-missile-defense/; Tong Zhao, "China Wants More Nuclear-Armed Submarines. Should Everyone Be Worried?," Carnegie–Tsinghua Center for Global Policy, October 22, 2018, https://carnegietsinghua.org/2018/10/22/china-wants-more-nuclear-armed-submarines.-should-everyone-be-worried-pub-77546.

1779 Massachusetts Avenue NW | Washington, DC 20036 | P: + 1 202 483 7600

CarnegieEndowment.org