CROSS-DOMAIN DETERRENCE IN US–CHINA STRATEGY

Workshop Proceedings

James Scouras | Edward Smyth | Thomas Mahnken

JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

CROSS-DOMAIN DETERRENCE IN US–CHINA STRATEGY

James Scouras

Edward Smyth

Thomas Mahnken

JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

Questions and comments regarding this document should be directed to:

National Security Analysis Department
The Johns Hopkins University Applied Physics Laboratory
11100 Johns Hopkins Road
Laurel, Maryland 20723

The views expressed in this document should not be construed as the views of any of the organizations with which the authors are affiliated.

CONTENTS

PREFACE

This study had its origin in a discussion between the director of the Johns Hopkins University Applied Physics Laboratory (JHU/APL), Dr. Ralph Semmel, and the former deputy assistant secretary of defense for nuclear and missile defense policy, Dr. Bradley Roberts, in June 2012. During that discussion, Dr. Roberts indicated he would be interested in JHU/APL-suggested approaches to thinking about cross-domain deterrence.

Consequently, JHU/APL initiated an internally funded study to address cross-domain deterrence. The Laboratory allocates a portion of its internal funding to a program of innovative research with the potential for significant impact on critical national challenges. This study, funded under that program, focuses on clarifying cross-domain deterrence issues and identifying productive research approaches. The first stage of the study culminated in a briefing provided to Dr. Roberts and his staff in January 2013. The Cross-Domain Deterrence Workshop, documented by this report, concludes the second stage of JHU/APL's research.

The study leaders are James Scouras (Principal Investigator), Edward Smyth, and Thomas Mahnken. Dr. Scouras is a national security studies fellow at JHU/APL. Mr. Smyth is the branch supervisor of the JHU/APL National Security Analysis Department's Analysis, Modeling, and Simulation Branch. Dr. Mahnken is a senior research professor of strategic studies at the Johns Hopkins University School of Advanced International Studies. Other JHU/APL researchers—notably Dr. Antonio DeSimone, Dr. Danielle Wood, and Mr. Michael Shehan—contributed cyber and space domain expertise to the study.

We are grateful to the experts who participated in the workshop, especially to the presenters and discussion facilitators, all listed in Table 1 of this report. In addition, we thank Margaret Harlow for taking notes and developing draft summaries of workshop sessions and Deborah Schlichting for managing the workshop logistics.

As the primary documentation of the JHU/APL Cross-Domain Deterrence Workshop, this report should be of interest to policy makers, analysts, and citizens concerned with emerging deterrence challenges, especially vis-à-vis China.

SUMMARY

This report documents the Cross-Domain Deterrence Workshop conducted on June 26, 2013, at the Johns Hopkins University Applied Physics Laboratory (JHU/APL) in Laurel, Maryland. The overarching objectives of the workshop were to identify: (1) the challenges in deterring actions in one domain of warfare (e.g., cyber, space, nuclear, conventional, etc.) by posing retaliatory threats in another domain and (2) research needs, and promising research approaches for advancing our understanding of these challenges and forging effective cross-domain policies and strategies.

For purposes of this workshop, we defined domains as categories of weapons effects—nuclear, conventional, space, cyber, missile defenses, chemical, biological, etc. Cross-domain deterrence, therefore, involves making retaliatory threats from one domain to prevent attacks from another. Because the topic of cross-domain deterrence is so broad, we limited our scope by both actors and domains under consideration. In particular, this workshop focused on China, which arguably poses the broadest array of cross-domain deterrence challenges. We further limited ourselves primarily to the nuclear, cyber, space, and conventional military domains.

The workshop sessions were Chinese Perspectives on Deterrence; Deterring Chinese Cyber Attacks; Deterring Chinese Attacks on US Space Capabilities; Deterring Chinese Nuclear Use; and Future Research. Here we present selected insights derived from workshop discussions, not session by session, but rather according to the following cross-cutting categories:

Deficiencies

- Available Chinese sources related to cross-domain issues are insufficient to confidently anticipate Chinese actions in a crisis or conflict.
- The United States lacks clear, effective, and commonly understood cross-domain strategies, especially for deterring and responding to cyber and space attacks.

Controversies

- Some participants argued that the Chinese leadership sees China's nuclear weapons as useful for deterring US retaliatory actions in several domains of warfare. Other participants argued that China sees its nuclear weapons as principally limited to deterring others' nuclear threats or use and conventional attacks highly threatening to Chinese Communist Party rule.

- Most participants believed it was important to develop a deep understanding of China's history, strategic culture, leadership, doctrine, and decision-making process. Others believed that we need only understand China's geopolitical circumstances, and logically analyze their options for actions in this context.

Needs

- The United States needs to place greater emphasis on denying benefits to both space and cyber attacks.
- The United States should try to strengthen international resolve against kinetic attacks in space and destructive cyber attacks.

Future Research

Future research topics include additional areas we need to understand about China and scenarios worthy of further analysis.

Understanding China

Several participants focused on understanding central aspects of China's strategic culture—its role in the international system, its values, and its fears. Other participants focused more directly on the need to understand China's approach to nuclear warfare and deterrence, deterrence of the strong by the weak, separating peacetime deterrence of the use of force and deterrence of further escalation during wartime or limited conflict, and coercive persuasion.

Scenarios

Many participants suggested scenarios involving combinations of actors in addition to those involved in a direct confrontation between the United States and China. Others suggested scenarios in which the internal situation in China is an important driver, scenarios involving a cyber attack that causes significant unintended damage, scenarios exploring reactions to nuclear use, and scenarios designed for developing and assessing options for responding in various circumstances. Several participants emphasized the importance of more realistically representing Chinese doctrine and decision making in scenario analysis.

Final Thoughts

In reflecting on the workshop discussions, we offer the following additional suggestions for avenues of future research. First, we might draw lessons that could be applied to emerging threats and future scenarios from studying the historical applications of deterrence in those situations in which multiple domains were in play. Second, we might also benefit from

comparative analyses of other states' perspectives and policies—particularly those of China and Russia—regarding deterrence, cross-domain and otherwise. Finally, our workshop was conducted at what can be characterized as a conceptual level. However, it became clear that considering cross-domain issues at an abstract level is limiting as almost all cross-domain deterrence decisions are context dependent. Thus, scenario analysis must be an integral component of future research. Moreover, as several participants noted, scenario analysis could greatly benefit from the analysts trying to emulate Chinese decision making.

1

WORKSHOP INTRODUCTION

This report documents the Cross-Domain Deterrence Workshop conducted on June 26, 2013, at the Johns Hopkins University Applied Physics Laboratory (JHU/APL) in Laurel, Maryland. In this chapter, we present the workshop objectives, discuss our approach to scoping workshop topics, clarify our usage of the terms *domain* and *deterrence*, and summarize the workshop read-ahead papers. We then present the workshop agenda, list workshop participants and their affiliations, and describe our approach to developing this report.

Objectives

The overarching objectives of the workshop were to identify: (1) the challenges in deterring actions in one domain of warfare (e.g., cyber, space, nuclear, conventional, etc.) by posing retaliatory threats in another domain; and (2) research needs and promising research approaches for advancing our understanding of these challenges and forging effective cross-domain policies and strategies.

Scope and Terminology

Because the topic of cross-domain deterrence is so broad, we limited our scope by both actors and domains under consideration. In addition, to facilitate dialogue, we established a definition of deterrence for use throughout the workshop.

Actors

Although a variety of actors could pose threats for which cross-domain deterrence may be useful, this workshop focused on China, which arguably poses the broadest array of potential threats for which cross-domain deterrence challenges appear most problematic. In particular, both the cyber and space challenges from China are relatively new and growing, with ill-defined norms of international behavior and poor visibility into China's strategic thinking and decision making.

In focusing on China, we recognize that cross-domain challenges from other states (and non-state entities) are not lesser included cases. That is, we should not expect that what we learn about China will necessarily apply to Russia, Iran, or others. These states need to be addressed as well, and comparative analysis of the various bilateral deterrence relationships might prove very informative.

We also do not consider non-state actors. These pose unique deterrence challenges that require an analytic approach that is different from that adopted for this workshop.

Domains

For purposes of this workshop, we have defined domains as categories of weapons effects—nuclear, conventional, space, cyber, missile defenses, electronic, chemical, biological, etc. Of these domains, space is somewhat of an outlier, as it is more commonly thought of as a place in which actions occur (the other domains of that ilk being land, air, sea, and cyberspace). However, one can think of weapons (both those based in space and elsewhere) that attack space capabilities (again, those based in space and elsewhere) as consistent with a domain characterized by a weapon effect. In any event, we recognize that continuing ambiguity in the

term *domain* remains an impediment to clear thinking and effective dialogue, but addressing terminology was not a focus of this workshop.

Also, we focused on military domains rather than on a whole-of-government approach to deterrence that would include the full spectrum of levers of national influence including trade, aid, diplomacy, etc. We emphasized the nuclear, cyber, space, and conventional military domains. Other important military domains, such as air and missile defenses, were only tangentially discussed. Similarly, military domains open to some adversaries but not to the United States (e.g., biological, chemical) were not addressed.

These choices were based on our judgments that the most challenging cross-domain issues arise in cyber and space and that isolating the nuclear domain remains a critical goal. Moreover, in thinking through cross-domain options, the conventional domain also looms large, given US superiority in that domain and its ability to scale effects. Nonmilitary domains are important, perhaps even central, to deter some cyber and space attacks, but their utility appears to be more relevant to threats at the lower end of the spectrum of violence.

Deterrence

For purposes of this workshop, we defined *deterrence* as the strategy that seeks to prevent actions by the specter of retaliation. That is, deterrence is only about sticks, rather than both carrots and sticks. Also, deterrence is about the anticipation of punishment rather than making actions more difficult to accomplish or mitigating their consequences. Notwithstanding other usages of this term, our usage is consistent with most dictionary definitions, including that of the Department of Defense.[1]

Cross-domain deterrence, therefore, involves making retaliatory threats from one domain to prevent attacks from another. Denial strategies also have their role in preventing unwanted actions, and, indeed, we explicitly addressed their utility in a number of questions posed during the workshop. However, for the sake of clarity, we do not define them as deterrence.

Finally, the workshop was conducted at the unclassified level, and—other than presentations—all comments were treated on a not-for-attribution basis. Presentation authors are identified on the workshop agenda, and presentation summaries in this report are associated with presenters.

[1] Department of Defense, *Dictionary of Military and Associated Terms*, Joint Publication 1-02, November 8, 2010, as amended through June 15, 2013.

Read-Ahead Papers

Two papers were provided to participants prior to the workshop. These were selected to ensure that all participants had a foundation of knowledge on cross-domain terminology and challenges and Chinese perspectives on deterrence. These papers, both by authors who also participated in the workshop, are summarized here:

Dean Cheng, "Chinese Views on Deterrence," ***Joint Force Quarterly***, **1st Quarter, 2011.** Mr. Cheng focuses on Chinese definitions related to deterrence and Chinese operationalization of deterrence theory, which differ in important ways from US definitions and practices, notwithstanding some fundamental similarities.

In terms of similarities, the core tenet that deterrence is based on the credible threat of use of military power is central to both Chinese and US theories of deterrence. Moreover, both sides recognize that credible threats require both military capability and the will to use that capability as judged by the side subjected to deterrent threats.

In China's application of deterrence theory, military capabilities include not only the traditional nuclear and conventional forces but also, increasingly, space and information capabilities. The roles of all these capabilities are evolving as technology advances:

- China distinguishes various levels of nuclear deterrence. Its strategy thus far has been one of "minimum" nuclear deterrence, in which a small number of nuclear weapons can retaliate against cities, but China may be edging toward "moderate" nuclear deterrence, which threatens a greater level of retaliation.
- Conventional long-range precision strike capabilities are increasing the importance of conventional deterrence.
- Space systems both support nuclear and conventional deterrence and can help neutralize an opponent's nuclear deterrent.
- Information capabilities support deterrence in their abilities to affect combat operations and influence leadership and public opinion.

While military capabilities are central to both US and China's theories of deterrence, China has a more expansive perspective on the capabilities that underwrite deterrence. In China's view, deterrence is based on all the components of "comprehensive national power," including military forces, economic power, diplomatic capabilities, and even political and cultural unity.

Another notable difference is that the Chinese term for deterrence, *weishe*, does not distinguish between deterrence (a strategy for preventing an unwanted action by using threats of retaliation) and compellence (a strategy for motivating adversary action, again through threats of harm),

whereas US deterrence theorists do. *Weishe* embodies both concepts as mechanisms for compelling an opponent to submit to the will of the deterrer.

Yet another significant difference arises in views of the relationship between deterrence and warfighting. In China, these concepts are seen as complementary. That is, deterrence extends into the combat phase of conflict to undermine the enemy's will to resist. By contrast, in the United States, the concepts are more separated—war is the consequence of deterrence failing.

Understanding these and other major differences in Chinese and US perspectives on deterrence can be enhanced by appreciation of the different histories and geopolitical situations of the two countries. Among the most important of these factors is the lack of a significant surprise-attack experience in China, analogous to Pearl Harbor; the lower level of concern in China with the lessons from World War I regarding inadvertent war; and the greater Chinese focus on multilateral deterrence as a result of threats from many states on its borders in contrast to the US bilateral deterrent focus as a result of its Cold War experience.

Vincent Manzo, "Deterrence and Escalation in Cross-Domain Operations: Where Do Space and Cyberspace Fit?" *Strategic Forum*, National Defense University, December 2011. Although this paper was published less than 2 years ago, it is one of the first to provide a comprehensive overview of emerging cross-domain deterrence issues, including alternative definitions of the term *cross-domain* and the applicability of concepts such as deterrence, proportionality, and escalation. Cross-domain challenges are illustrated using examples that focus on the roles of space and cyberspace in potential conflicts with China.

Mr. Manzo offers two alternative definitions of the term *cross-domain*.[2] In the first, the attacking platform uses a domain (air, land, sea, space, or cyberspace) that is different from that of the target platform (e.g., a land-based missile attacking a ship). In the second, the domain of the target is different from the domain of the intended consequences (e.g., attacking a satellite in space with intended consequences for sea, air, or land operations). By either definition, cross-domain deterrence has been commonplace in US strategy. However, increasing and asymmetric US dependencies on the space and cyber domains, coupled with new threats that exploit US vulnerabilities in these domains, have brought a renewed attention to cross-domain deterrence.

Long-standing principles of deterrence theory hold that the credibility of a retaliatory threat is enhanced if it is logically connected to, and has consequences that are proportionate to, the action being deterred. Currently, however, states lack a shared framework for how these

[2] Note that Manzo's definition of *domain* is not the same as that used in this workshop, and thus neither is his definition of *cross-domain*. The existing multiplicity of definitions is a clear indicator of the lack of a shared understanding of cross-domain issues among the US strategic community.

principles apply to attacks in the space and cyber domains. This undermines deterrence and increases the potential for misinterpretation that could lead to unintended escalation. Establishing such a framework is hampered by a lack of conflict experience in cyber and space relative to other domains, as well as differences in strategic cultures and asymmetries in objectives, strategies, forces, strengths, and vulnerabilities.

Manzo notes that even the internal US strategic community suffers from a lack of a common understanding, which hampers cross-domain deterrence and contingency planning. A necessary first step toward developing an inter-state framework is that the US strategic community engage in a comprehensive discussion of these issues, with the objective of developing a consensus that would facilitate integrating actions in space and cyberspace with those of the more traditional domains.

As a starting point for a shared international framework, Manzo offers the principle that, rather than focusing on the extension of conflict from cyber and/or space to the terrestrial domains as necessarily escalatory, "the real-world effects of such attacks, within the domain of the attack and in other domains, should determine whether they are escalatory and which responses would be appropriate." Among a myriad of other considerations that come into play, Manzo discusses the balance between offense and defense in various domains; the ability to substitute terrestrial for space capabilities; the international context of peace, crisis, or war; and the potential role and risks of ambiguity in US cross-domain deterrence strategy.

Agenda

The workshop was conducted at an unclassified level and on a not-for-attribution basis. The agenda appears below.

Cross-Domain Deterrence Workshop Agenda—June 26, 2013

9:00–9:30	**Workshop Introduction—James Scouras**
9:30–11:00	**Chinese Perspectives on Deterrence—Presentation by Thomas Mahnken**
	Discussion Facilitator—Edward Smyth
11:00–11:15	**Break**
11:15–12:30	**Deterring Chinese Cyber Attacks—Presentation by Stephen Blank**
	Discussion Facilitator—Antonio DeSimone
12:30–1:00	**Lunch**
1:00–2:15	**Deterring Chinese Attacks on US Space Capabilities—Presentation by Forrest Morgan**
	Discussion Facilitator—Alexander Ihde
2:15–2:30	**Break**
2:30–3:45	**Deterring Chinese Nuclear Use—Presentation by Michael Chase**
	Discussion Facilitator—James Scouras
3:45–5:00	**Future Research—Edward Smyth**

All sessions except the last were conducted as follows. First, a briefing was presented, with interactive discussion, to provide the foundation required to address cross-domain issues in general and the posed questions in particular. This was followed by a facilitated discussion of the posed questions, not all of which were discussed due to time limitations. In the last 5–10 minutes, participants provided computer responses to one or more of the posed questions. We anticipated that participants would gravitate toward answering those questions about which they were most knowledgeable.

Discussion Questions

Chinese Perspectives on Deterrence

- How much confidence can the United States have in its understanding of Chinese perspectives on deterrence, based upon existing literature?
- Is it an important issue that the United States and China have similar, yet different definitions, of deterrence?
- What misperceptions exist in China and the United States about each other's deterrence strategy?
- What do the Chinese think of the US discussion of "cross-domain deterrence?"
- China considers strategic deterrence to involve all elements of national power in a seemingly progressive pattern. How does this contrast with the US process?
- People's Liberation Army doctrine consists of both "deterrence campaigns" as well as "warfighting campaigns." Is this in contrast to US doctrine?

Deterring Chinese Cyber Attacks

- Can the United States effectively dissuade cyber attacks without demonstrating willingness to retaliate (i.e., are protection strategies and establishing behavioral norms sufficient for preventing cyber attacks?)?
- Are there effective retaliatory threats that stay within the cyber domain, or must retaliatory threats cross domains to be effective?
- What principles should guide the development of US cross-domain deterrence policies for cyber (e.g., are red lines useful, and, if so, what should they be and how should they be communicated?)?

Deterring Chinese Attacks on US Space Capabilities

- Can the United States effectively dissuade space attacks without demonstrating willingness to retaliate (i.e., are protection strategies and establishing behavioral norms sufficient for preventing space attacks?)?
- Are there effective retaliatory threats that stay within the space domain, or must retaliatory threats cross domains to be effective?
- What principles should guide the development of US cross-domain deterrence policies for space (e.g., are red lines useful, and, if so, what should they be and how should they be communicated?)?

Deterring Chinese Nuclear Use

- Does China share the US goal of isolating the nuclear domain?
- What US actions in other domains could provoke Chinese nuclear threats or use?
- What Chinese actions in other domains could provoke US nuclear threats or use?
- Do Chinese authors predict that their own or US precision conventional, cyber, or space attacks will elicit a nuclear response?
- Should the United States explicitly retain or relinquish the option to respond to cyber and space attacks with nuclear weapons, cultivate ambiguity, or be silent on the matter?

Future Research

- What else does the United States need to understand about China?
- Are there specific scenarios that should be examined?
- What has not been considered?

Participants

Participants, listed in Table 1, were drawn from academia, military war colleges, federally funded research and development centers and other think tanks, and industry. As workshop organizers, we tried to maintain a balance among the various disciplines required for cross-domain analysis.

Table 1. Workshop Participants

Participant	Affiliation
Acton, James	Carnegie Endowment for International Peace
Bishop, Christopher	The Johns Hopkins University Applied Physics Laboratory
Blank, Stephen	US Army War College
Chase, Michael	US Naval War College
Cheng, Dean	Heritage Foundation
DeSimone, Antonio	The Johns Hopkins University Applied Physics Laboratory
Evans, Dennis	The Johns Hopkins University Applied Physics Laboratory
Hopfinger, Patrick	The Johns Hopkins University Applied Physics Laboratory
Ihde, Alexander	The Johns Hopkins University Applied Physics Laboratory
Kauderer, Todd	The Johns Hopkins University Applied Physics Laboratory
Libicki, Martin	The RAND Corporation
Lieber, Keir	Georgetown University
Mahnken, Thomas	The Johns Hopkins University School of Advanced International Studies
Manzo, Vincent	Center for Strategic and International Studies
Mastro, Oriana	Georgetown University
Melcher, Gregory	The Johns Hopkins University Applied Physics Laboratory
Morgan, Forrest	The RAND Corporation
Nanos, G. Peter	The Johns Hopkins University Applied Physics Laboratory
Scouras, James	The Johns Hopkins University Applied Physics Laboratory
Smyth, Edward	The Johns Hopkins University Applied Physics Laboratory
Stokes, Mark	Project 2049 Institute

Approach to This Report

In publishing this report, our purpose is to provide a communication link between workshop participants and report readers. Thus, our approach can be characterized as minimalist. For each of the major sessions, we first summarize the oral presentations, including the discussions they generated. We next present edited computer responses, excluding only those inputs we judged not directly relevant to the question and those that added little insight (e.g., one-word answers). Finally, we group these responses into major themes, quoting participants extensively.

Once the draft report was completed, we sent it to all workshop participants for review and for clarification or elaboration of comments they had made during the workshop.

2

CHINESE PERSPECTIVES ON DETERRENCE

Our first session focused on Chinese perspectives on deterrence. There are at least three distinct reasons to study this topic. The most direct reason is that, because deterrence is a strategy that works in the minds of adversaries to influence decision making, we must try—to the extent feasible—to anticipate how our deterrence rhetoric and actions will play out in the minds of Chinese leadership and other audiences. Should that level of understanding prove imperfect, at a minimum our deterrence policies should reflect awareness of our limited understanding of Chinese perspectives. In either case, being aware of what we know and what we do not know can, at least in theory, help to support development of an effective deterrent by increasing the credibility of deterrent threats, preventing the misinterpretation of deterrence signals sent and received, and averting unintended escalation. Second, to the extent that Chinese perspectives on deterrence differ from those prevalent in the United States, we might gain a great understanding. Finally, understanding Chinese perspectives—starting with terminology and associated definitions—can facilitate international dialogue on these issues.

The first section summarizes the presentation on Chinese perspectives on deterrence provided at the workshop, followed by key questions and participant responses.

Presentation Summary: Chinese Perspectives on Deterrence

by Thomas Mahnken

Professor Mahnken gave a presentation on Chinese views of deterrence, drawn largely from Chinese military writings. He argued that Chinese military authors conceive of deterrence differently than strategic thinkers in the United States. Specifically, he noted that Chinese definitions of deterrence place a greater emphasis on coercion, and some varieties of deterrence include the use of force. In addition, he emphasized that the People's Liberation Army concepts of deterrence in each domain differ from those espoused in the United States, and People's Liberation Army concepts on the relationship between different domains also differ. This can be seen most starkly in the concept of "dual deterrence," which features the use of nuclear missiles to deter strikes and conventional missiles to launch strikes.

Definitions of Deterrence

Chinese definitions of deterrence differ from those of Western thinkers in several ways. First, Chinese concepts of deterrence are more active than those of Western strategists, emphasizing coercion as much as deterrence. For example, *The Science of Military Strategy* (2005) states, "deterrence plays two basic roles: one is to dissuade the opponent from doing something through deterrence, the other is to persuade the opponent what ought to be done through deterrence, and *both* demand the opponent to *submit to the deterrer's volition*."[3] Second, Chinese military authors view deterrence broadly, emphasizing the role of concealment, surprise, and psychological warfare. Third, in some instances, Chinese authors view the use of force as part of deterrence. For example, the authoritative *Science of Campaigns* (2006) states, "That is, we use strong military attack as the backing to create powerful deterrence, forcing the enemy to give up the attempt to resist."[4] Indeed, Chinese military theorists see deterrence and warfighting as dialectically unified.[5]

Chinese authors do not write about "cross-domain deterrence" as used in the US policy community. Chinese military doctrine does, however, contain discussions of "integrated strategic deterrence." As the authors of *The Science of Military Strategy* note, different countries have different means at their disposal to deter. China, for example, has nuclear weapons, conventional power, and a people's war capability. "By combining these means of deterrence, an integrated strategic deterrence is formed, with comprehensive national power as the basis,

[3] Peng Guangqian and Yao Youzhi, *The Science of Military Strategy* (Beijing: Military Science Publishing House, 2005); as cited in Dean Cheng, "Chinese Views on Deterrence," *Joint Force Quarterly* 60 (2011): 92.

[4] Zhang Yuliang, *Science of Campaigns* (Beijing: National Defense University Press, 2006), 203.

[5] Peng Guangqian and Yao Youzhi, *Science of Military Strategy,* 171.

conventional force as the mainstay, nuclear force as the backup power, and reserve force as the support."[6]

Chinese views of nuclear deterrence are operationalized in Chinese military doctrine. Specifically, the People's Liberation Army develops operational plans based on a series of canonical "campaigns." More specifically, People's Liberation Army doctrine includes "deterrence campaigns" as well as "warfighting campaigns." Deterrence and warfighting campaigns exist for both nuclear weapons and conventional ballistic missiles. Information operations are conceived of as elements of broader campaigns. Tasks include protecting campaign information systems, collecting intelligence, destroying enemy information systems, and weakening an enemy's ability to use information during war. As yet, however, there appears to be no independent campaign for the employment of space forces in Chinese doctrine.

Nuclear Deterrence

Chinese military writings link China's nuclear strategy to its status as the object of superpower nuclear threats. As the *Chinese Military Encyclopedia* states, "The nuclear weapons that China developed were done under coercion, in order to break the superpowers' nuclear monopoly, to oppose nuclear blackmail, for defense, and to guard the Chinese people against the threat of nuclear war."[7] In operational terms, the Chinese Second Artillery Force has traditionally thought of and planned for a number of deterrence and warfighting campaigns: nuclear deterrence, counter-nuclear deterrence (that is, resisting intimidation and coercion), and nuclear counter-attack operations. Since 1994, the Second Artillery has added a conventional mission, including conventional missile force deterrence operations, the conventional missile strike campaign, and support to joint operations.

The Second Artillery's *Science of Second Artillery Campaigns (SSAC)* outlines a set of deterrence campaign methods: (1) exert pressure through public opinion (information); (2) raise the level of weapons preparation; (3) demonstrate strength; (4) create momentum with troops—feints and simulated and real launches; (5) conduct launch exercises; (6) conduct nearby test launches; and (7) reduce the nuclear threshold. The concept of "reducing the nuclear threshold" is particularly important and refers to threatening nuclear escalation in the face of a conventional precision-strike campaign by a superior adversary in the following circumstances:

- "First, when an enemy threatens to carry out conventional strikes against our nuclear facilities (or nuclear power stations),

[6] Ibid., 177–178.

[7] Qian Gui and Shen Kehui, "Nuclear Strategy," in *Chinese Military Encyclopedia,* eds. Song Shilun and Xiao Ke, vol. 2 of 11 (Beijing: Military Science Publishing House, 1997), 244.

- "Second, when an enemy threatens to carry out strikes against our major strategic targets related to the safety of the people, like large-scale water and electricity stations,"
- "Third, when an enemy threatens to carry out medium or high strength conventional strikes against our capital, important nuclear facilities, and other political and economic centers,
- "Fourth, when conventional warfare continues to escalate and the overall strategic situation changes from positive to disadvantageous for us, and when national safety is seriously threatened, in order to force the enemy to stop its invasion and in order to save the country from danger."[8]

Conventional Deterrence

In 1993, the Central Military Commission assigned the Second Artillery the mission of "dual deterrence and dual operations," which emphasizes the importance of deterrence and combat roles for both the conventional and nuclear missile forces. The objective of conventional missile force deterrence operations is to influence the enemy's decisions by convincing them that China's missile force has powerful strike capabilities and that Beijing has the will to use them if necessary to prevent the enemy from challenging China's interests or to compel the enemy to accept Beijing's demands. Chinese authors write about conventional missile force deterrence operations of varying intensity, with associated activities, some of which include the use of force:

- Low-intensity conventional missile force deterrence "usually does not have a very strong confrontational nature." Its activities include:
  - Using the media to transmit propaganda about the missile force and changing the disposition of the conventional missile force units
  - Continuously improving the missile force's survivability, rapid response capability, ability to penetrate missile defense systems, and destructiveness
- Medium-intensity conventional missile force deterrence has a "definite confrontational quality." Its activities include conducting conventional missile force exercise launches.
- High-intensity conventional missile force deterrence has a "very strong confrontational nature." It is implemented through "close proximity or critical deterrence strikes," which involve firing missiles toward an area near an enemy state or into the waters

[8] Second Artillery Corps of the People's Liberation Army, *Science of Second Artillery Campaigns* (Beijing: People's Liberation Army Press, 2004), 294.

off of an enemy-occupied island to cause the enemy to feel an even greater sense of psychological pressure.[9]

Space Deterrence

Chinese views of space warfare and space deterrence have evolved in the last decade and a half. The entry on "Space Warfare" in the 1997 edition of the *Chinese Military Encyclopedia* viewed military operations in traditional terms, arguing, "Space warfare is an extension of warfare on the ground, at sea, and in the air; and the space force is an extension of the army, navy and air force. The emergence of space warfare will have a certain effect on wars of the future, but it will not play a decisive role. The primary factors for deciding victory and failure in war will remain the nature of the war and the support or opposition of the people."[10] The 2005 edition of *The Science of Military Strategy* portrayed space deterrence in considerably different terms, arguing that "it has great effects of shock and awe on the enemy." In the view of the authors, the means of space deterrence are flexible and include "interference, disruption, and destruction." They also note that space deterrence is restrained by international opinion, space law, and regulations.[11]

Information Deterrence

The use of information to deter or compel an adversary has been a feature of Chinese military thought for millennia. Indeed, the authors of *The Science of Military Strategy* (2005) invoke Sun Tzu in discussing the topic: "The best result information deterrence pursues is to 'subdue the enemy without fighting' (Sun Tzu) and strive for winning the victory of war by confrontation without shedding blood."[12]

Chinese authors see information operations as being launched at the beginning of a conflict and continuing throughout its course. They view their potential enemies, including the United States, as information dependent. They see information operations as a preemptive method that can be used to achieve information dominance. They believe that information operations will allow China to fight and win an information campaign, precluding the need for conventional military action.

---

[9] Zhao Xijun, *Coercive Deterrence Warfare: A Comprehensive Discussion of Missile Deterrence* (Beijing: National Defense University Press, 2005), 171.

[10] Yang Zhongcheng, "Space Warfare," in *Chinese Military Encyclopedia*, eds. Song Shilun and Xiao Ke, vol. 3 of 11 (Beijing: Military Science Publishing House, 1997), 602.

[11] Peng Guangqian and Yao Youzhi, *Science of Military Strategy,* 176.

[12] Ibid.

Chinese Perspectives on Deterrence: Key Questions and Participants' Responses

This section presents participants' perspectives on the agenda questions associated with the workshop session titled "Chinese Perspectives on Deterrence." The two sources of information for this section are (1) group discussions conducted immediately after the session presentation and (2) computer inputs provided at the end of the session.

Q How much confidence can the United States have in its understanding of Chinese perspectives on deterrence, based on existing literature?

Ten workshop participants addressed this question, with mixed judgments ranging from "minimal confidence" to "a pretty decent level of confidence." Although there was no consensus on the answer, the median view hovered in the neighborhood of "limited confidence."

One participant made a distinction between the academic, policy, and military communities:

- Academics might feel relatively more confident about US understanding of deterrence, but I doubt whether the policy or military communities feel this way. I certainly believe they should not feel confident about US insight into Chinese views.

Several participants focused on the facts that doctrine may evolve over time and some of the more important literature is somewhat dated:

- Some of the main published sources are from about 2000–2006. With some of these publications now 7–13 years old, it's worth keeping in mind that many things have changed since they were released, so we should definitely be on the lookout for new editions of some of the key sources and/or other new publications.
- It is hard to know how much a 10-year-old unclassified document, even if "authoritative" at the time it was published, accurately reflects the thinking of current top leadership in the Chinese government/military.

A number of participants cautioned against relying too much on doctrinal literature to predict Chinese actions in a crisis:

- Do China's leaders, themselves, really know when push comes to shove that they would do more, less, or the same as they hint they would do?
- People's Liberation Army doctrine will not, in the end, determine Central Military Commission decision making in the context of a future, hypothetical contingency.

- Doctrinal literature is just that—doctrinal literature. It discusses a lot of interesting things, but it doesn't necessarily describe how China would actually act in a real crisis or conflict.

Final points made were that the Chinese government is not a monolithic entity and that we have different levels of insight into different elements of the bureaucracy:

- While there is a significant body of literature published by the Academy of Military Science and the People's Liberation Army National Defense University and Second Artillery Corps, what do the People's Liberation Army General Political Department, the Central Military Commission General Office Research Bureau, and the Chinese Communist Party Central Committee General Office think about deterrence?

Q Is it an important issue that the United States and China have similar, yet different, definitions of deterrence?

Divergent views were evident from the eight respondents to this question. Half answered in the affirmative:

- This is absolutely critical due to the wide gaps [compared to US thinking] in Chinese thinking about many of the concepts that comprise deterrence (e.g., the role of nuclear weapons and proportionality, as well as many other aspects of deterrence).
- This issue is absolutely essential. Different concepts, different definitions, different cultures, and different histories shape and mold understandings and perceptions.
- Yes. The US focus is on capabilities, while the Chinese focus is on resolve. Investments by the United States in capabilities have value for deterrence only if the Chinese are convinced the United States has the will to act.
- To the extent that deterrence is based upon perception, the fact that the United States and China have differing definitions of deterrence matters a great deal. To cite one example, China might launch a missile in close proximity to US naval forces as a deterrent signal, whereas the United States might view such an act as one of aggression.

The other half of the respondents acknowledged differences in US and Chinese definitions of deterrence but questioned the significance of these differences:

- Yes, but I think the differences are sometimes exaggerated.
- Not necessarily. It is not important where the United States and China draw the borderline between "deterrence" and "coercion," provided the United States understands

Chinese viewpoints and has an approximately accurate ability to know what they would do in a crisis and an ability to predict how willing they would be to initiate a crisis.

- Too much is made of perceived differences between US and Chinese definitions of deterrence. For one thing, definitions are just definitions. However, more importantly, I suspect US and Chinese views are quite similar, controlling for differences in strategic position. For example, the Chinese likely think of nuclear use in ways far more similar to the United States than one might conclude from public debates about China's "no first use" policy.
- Yes, but I'm not certain of the ramifications. The Chinese view of "correlation of forces" as ultimately determinative is not the same as the Western notion of matching ends and means or stopping at less than ultimate victory in the pursuit of long-run stability.

Q What misperceptions exist in China and the United States about each other's deterrence strategy?

The motivation for this question is the concern that misperceptions about each other's deterrence strategy could inadvertently lead to conflict and/or conflict escalation. Misperceptions identified by participants focused on identity, motivation, and the potential for escalation:

- One critical issue is that, in a major conflict, both the United States and China could perceive themselves as the "defender," with the consequence that escalation would become more likely and harder to control. This is reflected in the language used by each side to describe capabilities to hinder US freedom of access; the United States calls them "anti-access/area-denial capabilities," while China calls them "counter-intervention capabilities." More generally, China views its buildup as defensive and the goal of reunifying Taiwan as correcting an historical injustice. The United States worries the buildup is offensively oriented and would view an attempt to seize Taiwan by force as offensive. This is a recipe for escalation.
- Some Chinese general officers still think that the goal of the United States is to destroy them. This was shockingly apparent when a group of Chinese generals and colonels from their nuclear rocket forces met with Department of Defense personnel in 2008 or 2009.
- I think US civilian and military planners misperceive the degree to which AirSea Battle will trigger Chinese escalation. I think Chinese leaders misperceive the willingness of the United States to engage in military conflict in East Asia over issues that China perceives as nonvital/nonstrategic to the United States. Paradoxically, the Chinese

also probably misperceive US willingness to revise the status quo (i.e., they probably believe that we have more aggressive/revisionist designs than we have).

- Many misperceptions exist (e.g., under what conditions would each side go nuclear, how nuclear weapons deter reprisals for conventional or information warfare strikes, what constitutes a first strike, etc.).
- Misperceptions exist regarding issues of resolve and controllability of escalation and crisis management. Do crises develop momentums of their own? It is unclear whether the Chinese fear loss of crisis control as much as the United States does.

One participant noted the difficulty faced by China due to multiple voices in the United States:

- The Chinese have a hard time separating official US policy and what they may infer from statements by US media, congressmen, lower-level US officials, or Defense Science Board reports.

Q What do the Chinese think of the US discussion of "cross-domain deterrence"?

No respondent identified any Chinese mention of the US discussion of cross-domain deterrence:

- I am not aware of any Chinese reactions to US discussion of cross-domain deterrence.
- I haven't read anything yet in Chinese literature about this.

Some explained China's thinking without reference to the US discussion:

- China considers strategic deterrence to involve all elements of national power in a seemingly progressive pattern. How does this contrast with the US process? China's view incorporates all elements of national power and, unlike ours, elides the difference between peace and war.
- Chinese writings suggest that they believe in cross-domain deterrence. I would suggest the focus is not "cross-domain," but that it is holistic—deterrence across domains, but deterrence isn't stovepiped to begin with.
- My impression is that it isn't thought of as a separate concept. From the perspective of a weaker power, asymmetry is the goal. The ability to leverage capabilities in all domains to inspire the desired effect is a given. Cross-domain deterrence may be considered more robust only because employing multiple domains could be considered a force multiplier (i.e., more effective militarily), and therefore, the threat of it should enhance deterrence.

One respondent took note of the incoherence of thought in the United States about cross-domain deterrence and, by implication, the difficulty China would have of making sense of it:

- I wonder if *anyone* could coherently identify or summarize the US discussion of cross-domain deterrence.

Q China considers strategic deterrence to involve all elements of national power in a seemingly progressive pattern. How does this contrast with the US process?

Most respondents' comments suggested that Chinese conceptions about deterrence are both broader and more integrated than those of the United States. By contrast, most thinking in the United States about deterrence focuses on the nuclear domain:

- It would be great if the United States had a coordinated, whole-of-government approach to strategic deterrence, but it doesn't. The United States has in recent years assigned "deterrence" to combatant commands, where it is dealt with variably.
- US leaders tend to think of deterrence in a more compartmented fashion, focusing mainly on nuclear. This wasn't always true, of course. Throughout most of the Cold War, the United States used threats of nuclear retribution to deter a Soviet conventional attack on Western Europe. In the post-Cold War era, however, US leaders have largely assumed that the country's conventional forces would prevail in any war it chose to enter. Consequently, they have given much less thought to deterring conventional attacks. They have also attempted to segregate nuclear threats and marginalize them in international discourse, believing such actions reduce risks of nuclear war and pressures for nuclear proliferation. Chinese and Russian leaders, however, see such moves as thinly veiled attempts to secure US advantages in conventional warfighting. Consequently, they do not accept this strict segregation. Just as when the United States believed itself conventionally vulnerable, China and Russia have turned increasingly to integrating their nuclear and conventional deterrence concepts.
- Too often, in the United States, deterrence is meant to be nuclear.
- For China, national power is not progressive. It is much more holistic. It is not politics to diplomacy to economy to military. It is, as the Chinese say, a matter of "comprehensive national power."
- The United States is more likely to separate the various notions of deterrence and limit "strategic deterrence" to nuclear war. However, it is unclear what difference this distinction makes.

Two respondents did not see a difference or thought suggested differences may be exaggerated:

- Both the United States and China regard deterrence as involving all aspects of national power in a somewhat progressive manner.
- The United States casts China in some sort of idealized light, believing that all its strategies and policies are integrated while ours are stovepiped. People commented on US resolve, but Chinese resolve (China's willingness to act and disregard the effectiveness of US and world responses) should also be considered.

Q People's Liberation Army doctrine consists of both "deterrence campaigns" as well as "warfighting campaigns." Is this in contrast to US doctrine?

Respondents identified the following differences between US and Chinese doctrine:

- The United States does not really think about campaigns quite the way the Chinese do; in other words, it doesn't have a "joint blockade campaign" or "anti-air-raid campaign." So there is a contrast, but it is broader than the distinction between deterrence actions and warfighting campaigns.
- China's concept of active deterrence is similar to Schelling's concept of suggestive escalation and threats that leave something to chance—using force, perhaps against a tactical target, primarily to influence the adversary's perceptions (e.g., to deter escalation or increased involvement in the conflict). This concept has soaked into US thinking about limited nuclear strikes.
- Chinese doctrine is more blurred, perhaps because of less concern about the inability to sustain crisis management.
- The United States thinks about deterrence as a "Phase 0" problem. It also does not integrate deterrence and warfighting to the extent that China does.

One respondent emphasized similarities over differences:

- I think observers tend to exaggerate the differences here. The United States tends to talk about military planning and force requirements for the purpose of deterrence and, if deterrence fails, for mitigation (which essentially means warfighting). The fact of the matter is that warfighting military capabilities are arguably the key building blocks of deterrence, and this is recognized by both US and Chinese leaders.

3

DETERRING CHINESE CYBER ATTACKS

Deterring Chinese cyber attacks is, arguably, the most daunting of the cross-domain challenges facing the United States. This is due to the confluence of several phenomena, in addition to the oft-cited asymmetric US dependence on cyber for both military and civilian applications and the difficulties with attribution of cyber attacks. First, cyber is the newest domain of warfare and, as such, lacks the maturity of thinking that has been applied to many other domains of warfare, particularly the nuclear and conventional domains. In addition, cyber intrusions (as opposed to attacks that cause tangible damage to systems or people) have become commonplace, creating a precedent that makes establishing contrary norms of behavior far more difficult than, for example, in the space domain, which has, since Sputnik, enjoyed the norm that peacetime attacks on satellites are neither expected nor acceptable behavior. Finally, there is little experience with cyber attacks that would establish a solid basis for expectations regarding retaliation.

The first section summarizes the presentation on deterring Chinese cyber attacks provided at the workshop, followed by key questions and participant responses.

Presentation Summary: Responding to Chinese Information Warfare

by Stephen Blank

Dr. Blank's presentation is based on a draft paper supplied in advance to workshop participants.[13] He first discussed Chinese perspectives regarding the nuclear, conventional, cyber, and space domains, emphasizing the inherently cross-domain nature of Chinese deterrence strategy and military operations planning. After a brief discussion of new Chinese doctrinal concepts, he concluded with suggestions for counteracting approaches that the United States can take to enhance deterrence and prevail in war should deterrence fail.

Chinese Domain Perspectives

Nuclear

China uses nuclear weapons as a shield for its information warfare and other preemptive offensive operations (or, as China describes such actions, "active defense") by deterring retaliatory attacks in all domains—nuclear, conventional, and even information warfare. Just as every element of national power is seen by China as contributing to deterrence, China's nuclear deterrence applies to all forms of enemy retaliatory action. For example, consider a scenario in which China executes a cyber attack that knocks out US satellites. China might well brandish nuclear weapons to deter conventional or information warfare reprisals.

Thus, nuclear deterrence is inherently a cross-domain form of deterrence. This assessment is based on an analysis of literature by American, Indian, and Chinese authors, as well as consideration of points of similarity with Russia, where conventional attacks on, for example, command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) would clearly provoke a nuclear response.[14]

An important implication of China's strategy of using nuclear weapons to deter attacks from other domains is that Chinese proclamations about no first use cannot be relied on.

Conventional

Regarding the conventional domain, it is important to recognize that informational capabilities now permeate all Chinese military operations in land, air, sea, and space. They are now approaching the point where conventional operations are inherently cross-domain. Just as

[13] Stephen Blank, "Responding to Chinese Information Warfare" (unpublished, US Army War College, 2013).

[14] One participant cautioned that many experts believe China is still focused on nuclear weapons as deterring only, or primarily, nuclear use.

it has made the United States vulnerable, growing reliance on informational capabilities to support conventional operations is now also making China vulnerable to information warfare.

Information Warfare

Chinese views on information warfare differ in important ways from those of the United States. Similar to nuclear weapons, and unlike the United States, China views information warfare as providing a form of deterrence against all manner of enemy reprisals—informational, conventional, and even nuclear. Computer network attack is the spearpoint of this deterrent.

While both the United States and China use information warfare in Phase 0, the United States sees peace as one thing and war as something completely antithetical, in contrast to the Chinese perspective of a much more seamless connection between peace and war. Thus, the Chinese view Phase 0 information warfare as part of intelligence preparation of the battlefield and as including perception management on a grand scale. It is also very possible that China sees information warfare as an assassin's mace—a weapon that can strike suddenly and decisively to overcome an enemy's strength.

Space

Space is of increasing importance to China, as evidenced by anti-satellite activity; civilian space efforts; and support of conventional military capabilities to wage information warfare, launch strikes to target submarines, for example, and deter enemy strikes and counterstrikes against Chinese space and other systems. This reinforces the conclusion that Chinese military operations, like those of the United States, are inherently cross-domain and becoming more so over time.

Cyber, space, air, and naval capabilities are increasingly organically linked and interdependent; thus, a successful information warfare campaign could seriously degrade military capabilities. Both sides are increasingly reliant on cross-domain operations and vulnerable to information warfare campaigns intended to impede and degrade the other side's operations.

New Doctrinal Concepts

There are new Chinese doctrinal concepts developing, which reinforce the inherently cross-domain nature of military operations. Integrated electronic warfare pulls together all operations utilizing information warfare against enemy targets. Closely aligned with the People's Liberation Army's doctrine for fighting local warfare for limited objectives under informatisized conditions, this doctrine calls for a fully networked architecture capable of coordinating military operations in all domains and across the electronic spectrum, including electronic warfare attacks on enemy C4ISR networks and computer network attacks on information networks.

A related Chinese concept, known as "systems sabotage warfare," involves degrading the enemy's C4ISR to such a degree that it will lack the capability or the will to resist Chinese operations. This concept is more evidence of inherently integrated activities across the electromagnetic spectrum and all domains.

How Should the United States Respond?

Given that the Chinese have made it clear that they seek to prevail in localized warfare for limited objectives under informatisized conditions, how should the United States respond? First, the United States must make clear to China that any such conflict involving US interests and allies, or the United States itself, would be prolonged. China fears internal security tensions (social and ethnic unrest, economic slowdown, etc.) more than external threats. A prolonged war would aggravate these domestic tensions. For example, actions such as an oil blockade in the Malacca Strait, while not necessarily the answer, could prolong a conflict and aggravate domestic economic and political tensions in China.

Second, the United States must also invest in robust and redundant US and allied conventional, space, missile, and cyber defenses. Such a capability would make it difficult for China to seek a quick victory. In addition, it would also help the United States to prevail in a prolonged war and thus would also enhance deterrence of China. For example, China may well be miscalculating the impact of cyber strikes on US or allied targets. It is unclear whether Chinese threats of cyber strikes alone, even if they are "overwhelming," would deter adversaries. However, in any event, robust cyber defenses would send a signal that not only can the United States prolong the war, but Chinese cyber threats would not deter US and allied responses.

Taking this one step further, beyond working with allies to develop an Asian–Pacific intelligence, surveillance, and reconnaissance (ISR) capability, the United States could also work to develop an information strike capability. While this might provoke a reaction from China, it should reinforce the perception that China will not be able to achieve a quick victory.

Third, the United States needs to be able to conduct offensive conventional strikes on Chinese ISR capabilities. However, there is an inherent danger in this approach. Although offensive conventional strikes may be successful in wartime in crippling Chinese military capabilities, such strikes could provoke China into escalation that would lead to nuclear war.

Strikes of C4ISR targets, especially, could well meet the criteria to abandon China's policy of no first use. It is clear from Russian doctrine that striking such targets would meet the Russian criteria. Given the contemporary strategic environment, systematic large-scale attacks on C4ISR could lead to an escalation at the nuclear level. Therefore, there is an inherent cross-domain risk in those attacks. This could be true for both sides, and the Chinese may not be fully aware that they are playing with fire.

Fourth, the United States needs to look to diplomacy to complement military actions and responses. Together with allies, the United States should develop/build a network of relationships and capabilities to enhance ISR and deter Chinese probes. The United States also needs to include cyber issues (as well as cross-domain and nuclear) as part of military discussions with China, just as nuclear issues have been discussed with Russia for the past 55 years. China needs to understand the United States better, just as the United States needs to understand China better.

Finally, the United States should agree with Russia that there will be no subsequent strategic arms reduction talks without including China. Having the Chinese involved in such a discussion would (1) force discussions of strategic contingencies; (2) create a process to develop mutual understanding over time; (3) stop China from being a free rider on the superpowers; (4) reduce opacity in Chinese nuclear capabilities and plans; (5) politically, drive a wedge between Moscow and Beijing; and (6) bring everyone into a more secure and regularized relationship.

Deterring Chinese Cyber Attacks: Key Questions and Participants' Responses

This section presents participants' perspectives on the agenda questions associated with the workshop session titled "Deterring Chinese Cyber Attacks." The two sources of information for this section are (1) group discussions conducted immediately after the presentation and (2) computer inputs provided at the end of the session.

Q Can the United States effectively dissuade cyber attacks without demonstrating willingness to retaliate (i.e., are protection strategies and establishing behavioral norms sufficient for preventing cyber attacks?)?

Two respondents based their answers on a fundamental tenet of deterrence—if there is nothing to be gained by attacking, there is no motive to attack and thus no need to threaten retaliation to deter an attack. However, these respondents appear to differ on the likelihood of achieving defenses that can achieve the necessary level of protection. The first sets a very high standard—defenses must be "virtually impenetrable"—and implies that such a standard is impossible to meet:

- No. Unless US cyber defenses are virtually impenetrable, to deter a cyber attack, the perpetrator must be at risk of losing something that it already has.

The second respondent set a more ambiguous standard—defenses must be "good enough"—and implied that such defenses might be feasible:

- If your defense is good enough, it doesn't matter that someone else is attacking. In the long run, sufficient levels of frustration on the attacker's part may dissuade them from investing in their search for vulnerabilities in your systems.

Several respondents emphasized that the answer to this question turns on the meaning of "attacks." Attacks that cause damage to either military capabilities or civil infrastructures must be distinguished from cyber espionage intended to exfiltrate data and other forms of cyber intrusion. These respondents agreed that retaliatory threats would be necessary to deter cyber attacks but might be inappropriate or inadequate against cyber intrusions.

- It is important to distinguish between cyber attacks aimed at inflicting actual damage and cyber espionage. Espionage is to be expected and probably should not provoke retaliation against a foreign country.

  How could you deter a cyber attack without demonstrating a capability and the will to retaliate? Computer network defense and norms alone seem unlikely to be enough or at least not without some threat of retaliation in kind or through some other means.

  How could cyber espionage be deterred? It probably cannot be deterred with defenses, and threat of retaliation in kind will not help if the other party assumes similar activity is already underway. Norms might have a role but would require agreement between the parties about the norms that would be appropriate. Maybe other means—economic or diplomatic consequences, most likely—could influence China's decision calculus and deter at least some types of cyber espionage (such as theft of intellectual property and confidential business information from US companies).
- This is a really tough question, especially given the ambiguity of what "cyber attacks" might actually entail. I don't think a "demonstrated" willingness to retaliate is necessary for effectively dissuading cyber attacks on US military systems and capabilities that would effectively cost US lives or undermine military missions during a conflict. They should expect that retaliation. However, if the goal is deterring the kinds of cyber attacks that have already occurred (i.e., largely of the espionage type), the United States would need to dramatically ramp-up its own offensive cyber operations against Chinese targets and do so in a way that clearly conveys that such actions are explicitly retaliatory (and even escalatory).
- Yes, but only if the United States can demonstrate a consistent ability to promptly detect and defeat attacks and close the gaps through which they came without suffering degraded operational capabilities. Opponents can launch cyber attacks with very low

costs to themselves. Therefore, the main cost–benefit calculation opponents have to consider is whether the degradation in US operational capability (or the value of cost imposed on the United States) would be great enough to offset the attacker's cost in terms of the loss in intelligence exploitation it had been enjoying in the targeted system up to the point of the attack. If the United States can make defenses and forensic capabilities sufficiently responsive and reliable to deny an opponent's benefits and promptly close off access, then calculating state adversaries will not attack. The United States will still be plagued by hacker groups and others just interested in causing trouble, but serious threats will be deterred.

One respondent emphasized that cyber attacks are most likely to occur not in isolation but as part of a larger conflict, and that the effectiveness of deterrence should be considered in that broader context:

- A cyber attack is likely to occur as part of a broader attack. Demonstrations of resolve and willingness to retaliate to an attack more generally should dissuade cyber attack as a subordinate element of such an attack.

One respondent thought that only demonstrated protection and recovery capabilities would be effective, while another thought that only retaliation would be effective:

- It depends what you believe about how China thinks about using cyber. I don't think the Chinese are thinking of it to deter (i.e., to threaten use of cyber to harm the opponent to convince the opponent not to take some action). I think China thinks about using cyber to reduce US military effectiveness—to degrade, delay, deny, etc., US use of force. If this is true, the best way to deter Chinese cyber attacks is to demonstrate (1) the United States can operate with limited C4ISR; (2) if it can't, it will wait until it is back online and then act; and (3) the United States can protect itself. I think behavioral norms won't help, and US ability to retaliate with cyber won't do it either.
- Obviously not. Current thinking concludes that the United States is not capable of protecting its society against a severe information attack, and such robustness is years in the future, if it is possible at all. Because of the challenges related to attribution, US unwillingness to agree to international norms, and the newness of the technology, international behavioral norms have not arisen and are not likely to be codified in the near future. In the international community, it is expected that the United States retaliates in kind to attacks—disruption for disruption, loss of life for loss of life. The expectation that the United States would conduct such an attack in retaliation serves as deterrence.

Q Are there effective retaliatory threats that stay within the cyber domain, or must retaliatory threats cross domains to be effective?

Most respondents thought that limiting retaliatory threats to the cyber domain would not be effective in deterring cyber attacks, largely due to asymmetric US dependency on information systems. One respondent emphasized that, with greater understanding of Chinese perceptions, ambiguity regarding China's potential response to a cyber attack could work to the US advantage:

- Because the United States is more reliant on cyber capabilities than China, it seems unlikely that, in general, US responses could be effective deterrents if they were limited to the cyber domain. That said, the United States is not—and in practice almost certainly will not be—specific about how it will respond to cyber attacks. For this reason, the real challenges are (1) understanding how China thinks the United States would respond to a cyber attack and (2) understanding how to shape Chinese perceptions in a direction favorable to the United States.

As with the previous question, some respondents distinguished between cyber espionage and cyber attacks:

- To deter cyber espionage, the United States could improve defenses or reduce the value of the information that is collected by feeding the intruders disinformation, *but* I think you probably have to go across domains—into the economic and diplomatic domains, in particular—to have much of an influence on the other side's decision calculus. To deter cyber attacks, threat of retaliation in kind might be perfectly sufficient, at least for some types of attacks.

Again, similar to the previous question, several respondents emphasized that cyber attacks are likely to occur in the context of a broader conflict, with the implication that responses need not be constrained to the cyber domain:

- Because cyber attacks are unlikely to occur on their own, retaliation is likely to occur in the context of a larger conflict.
- Because an attack is unlikely to be one-dimensional, retaliatory effects need not be one-dimensional as well.
- There could be proportional or equivalent cyber retaliatory strikes in peacetime, but during an actual war, the United States may well have to employ cross-domain retaliation because, on both sides, all military operations either are cross-domain or are increasingly becoming cross-domain.

Respondents raised a variety of issues with limiting responses to the cyber domain. Among them were the US offensive cyber capability and the level of confidence the United States can have in it:

- I do not think retaliatory threats "must" cross domains to be effective, but the question of whether there are effective retaliatory threats that stay within the cyber domain turns on technical questions about US offensive cyber capabilities and the degree of damage the United States can inflict on Chinese systems and capabilities.
- In principle, cyber retaliation could deter a cyber attack, but the United States would need to be able to inflict serious damage on a perpetrator through cyber retaliation. In practice, it is uncertain that the United States can be confident of such a retaliatory cyber capability, so it needs to consider non-cyber approaches (to include economic penalties against a nation-state that institutes a cyber attack).

One respondent noted the relationship between the damage that would be inflicted by a retaliatory threat and the credibility of that threat:

- A same-domain retaliatory threat produces weaker effects (or at least no stronger effects), but it is more credible than a threat that would have the United States respond with kinetic weapons to a non-kinetic attack. It comes down to the question of whether adversaries think the United States wants to go to war over an attack that does not kill anyone.

Several respondents focused on the issue of proportionality:

- While it is likely that US retaliation for a cyber attack would be cyber related, this is not guaranteed. However, the impact of the retaliation should be similar to the kind of effects suffered by the United States. Examples of acceptable retaliation to a cyber attack that caused a blackout in a major US city that lasted 24–48 hours include a US attack that achieved similar results conducted through agents/proxies or a cruise missile against a power distribution station.

Q What principles should guide the development of US cross-domain deterrence policies for cyber (e.g., are red lines useful, and if so, what should they be and how should they be communicated?)?

Respondents discussed a wide variety of principles involving red lines, proportionality, ambiguity, attribution, targets, and cooperation:

- Red lines could be credible if they are communicated both openly and privately and then upheld by action in response to active probes. The United States would have to make clear which targets or kinds of attacks are "off limits." It should also make clear that it will retaliate against attacks.
- Maybe the United States could make a distinction between tactical targets that support military operations (the power to an air defense radar) and strategic or critical infrastructure targets (the power to a city) and persuade others to agree that the former is a legitimate military target while the latter should be off limits.
- The United States must make it clear that a cyber attack aimed at inflicting serious damage (e.g., crashing the electrical grid or the stock market) will be treated the same as a conventional attack using a cruise missile, especially if such an attack succeeds. By contrast, cyber espionage needs to be treated as consistent with expected international behavior, and the primary response should probably be defensive. Of course, the preceding discussion assumes the United States knows who took down its electrical grid through a cyber attack. Unless the attack occurs in conjunction with some sort of broader war, it may be very difficult to know for sure who conducted the attack.
- The United States should first develop a concept of how cyber warfare is likely to occur, in what form, and in what relationship to larger conflict before it starts talking about red lines. That being said, deterrence is often enhanced by uncertainty ("the threat that leaves something to chance").
- Say nothing explicit. The United States does not have the attribution capability to guarantee a response, and it does not have a history of response to convince others that it failed to respond due to a lack of understanding, rather than a lack in motivation to retaliate.
- An eye for an eye, a tooth for a tooth would probably work as well for developing cross-domain deterrence policies as anything else. That is to say, this principle would be both more credible and more effective than attempting to convey a more escalatory threat. For example, if the United States wants to deter Chinese cyber attacks that undermine real US military effectiveness, cost US lives, or destroy critical

infrastructure, threatening cross-domain strikes against Chinese military targets would seem reasonable, credible, and probably the most effective strategy for deterring those attacks in the first place. Issuing those threats to deter continued espionage would not be an effective strategy.

- Actions such as deepening and broadening cooperation with Taiwan in the cyber domain—a bilateral "cyber coalition"—could impose a cost on Chinese cyber operations. Cyber cooperation includes intelligence sharing, a combined computer emergency response center, synchronization of information and communication technology policy, etc.

4

DETERRING CHINESE ATTACKS ON US SPACE CAPABILITIES

Deterring Chinese attacks on US space capabilities has become a more urgent concern with China's recent successful anti-satellite test. The United States is highly dependent on space assets for the effective functioning of its military, including both conventional and nuclear capabilities. Although China is also becoming more dependent on space, the large asymmetry in space dependency endures. At the same time, little attention has been paid to making satellites less vulnerable, increasing the robustness of constellations of satellites, and maintaining terrestrial alternatives to space capabilities. Moreover, since Sputnik, while the precedent of unfettered overflight of national territory by satellites has become ever more firmly entrenched in practice, as a matter of policy, China does not accept this norm. Thus, in the search for strategies to protect US space assets, cross-domain deterrence looms large, albeit highly problematic.

The first section summarizes the presentation on deterring Chinese space attacks provided at the workshop, followed by key questions and participant responses.

Presentation Summary: Deterring Chinese Space Attacks

by Forrest Morgan

Dr. Morgan first conceptualized space deterrence as a stability issue, then provided relevant principles of deterrence and applied them to the issue of deterring Chinese threats to US space capabilities. He concluded with recommendations on developing a national space policy, making threats of retaliation more credible, and enhancing the ability to reduce benefits of an attack to an adversary.

Conceptualizing Space Deterrence as a Stability Issue

Deterring attacks on space assets is to some degree a first-strike stability issue. In the late Cold War, the United States thought of the first-strike stability problem in a game theoretic framework: if neither side can manage escalation once nuclear war breaks out, both sides are motivated to strike first and do as much damage limitation as early as they can. While space is not exactly that world, there will be relatively few and weak firebreaks against rapid escalation if conflict breaks out in space.

Deterrence in space and in the terrestrial domain are interdependent. An earlier RAND study concluded that the United States can deter attacks in space in peacetime when it does not need to, and it cannot during wartime when it does, so deterrence has no value. However, the United States should not think exclusively in terms of space deterrence. The real issue involves the critical threshold between peace and war: what role does deterring others from attacking the United States in space play in raising that threshold to a higher level, so we do not go from peace to war? That is ultimately a cross-domain issue.

To illustrate, if China is at the brink of war with the United States and it thinks it can succeed in the terrestrial environment by going after the United States in space, and the United States cannot deter China from that course of action, China is more apt to cross that threshold. However, if the United States can structure the international environment and US space architectures such that when China looks at the cost–benefit trade-offs, China decides that attacking the United States in space is a higher threshold than it wants to cross, then when it looks at attacking in the terrestrial environment, it will realize it would have to fight a US conventional military force with full transformational capabilities fully supported by space capabilities. As a result, the threshold of that decision is raised as well. So deterring space attacks is a critical cross-domain challenge for general deterrence.

Fundamentals of Deterrence

Deterrence is about manipulating a potential adversary's decision calculus about whether to launch an attack or not. An effective deterrent will persuade an adversary that the probable costs of an attack are likely to exceed the probable benefits. To create this perception, the United States can either raise expectations of cost via threats of punishment, lower expectations of benefits via defenses, or both. Deterrence and defense, done right, are mutually reinforcing.

If deterrence involves only military threats of punishment, rather than including protection as well, the decision space narrows down to mainly nuclear deterrence because the cost of executing those threats is so high it will give the adversary dramatic pause.

The history of conventional deterrence is a very different story. It is very difficult to deter an adversary from attacking by using threats of conventional punishment. Look at Slobodan Milošević in Serbia. Look at Saddam Hussein in Iraq. Deterrence failed in these cases because the adversary thought he could withstand conventional punishment long enough to achieve his military or political objectives or get someone to intercede on his behalf. In the conventional world, in the broader scope of history, as opposed to just the nuclear age, deterrence has been mainly about defense.

Applying Deterrence Principles to Chinese Attack on US Space Capabilities

Deterring attacks on space assets is more like conventional deterrence than nuclear deterrence. It is really hard to deter an adversary by threatening to impose costs.

Adversaries will attack selected space capabilities in selected ways to create operational effects (interdict US force enhancement capabilities for US transformational warfighting forces in the terrestrial environment). For example, adversaries could attack reconnaissance to make it hard to target mobile forces; strike communications to affect US networks; interdict GPS signals to affect US precision-guided weapons, etc. The key question the adversary will ask is whether attacking assets in space makes its terrestrial military operations more effective.

During the early portion of the Cold War, the United States had a tacit understanding with the Soviets not to interfere with each other's space assets, except on the margins. However, both sides then used space assets mainly to support their national strategic (i.e., nuclear) missions. After the sobering effects of the Cuban Missile Crisis, the United States realized that stability was better than fighting a nuclear war; therefore, it did not want to do anything to its space assets that created the perception that it might be about to initiate a nuclear war.

The situation has changed over the years, though. In the last several decades, the United States has progressively used space assets to support US conventional terrestrial military forces and do so in a way that has made US forces very intimidating to potential adversaries. As a result, the People's Liberation Army might find attacking US space assets an attractive option in efforts to "level the playing field" by reducing US warfighting capabilities.

It is not just that China is developing a counter-space capability to defeat the United States in war. Demonstrating the ability to attack in space contributes to China's ability to deter US intervention in the western Pacific. China is developing and demonstrating counter-space capabilities to let the United States know what it is up against if it comes to a fight—that it is going to take some losses in US space assets. That will raise US costs in terms of casualties and losses; therefore, the United States had better take that into consideration in its weighing of costs, benefits, and stakes in deciding whether or not to intervene in, for example, a Taiwan crisis.

How Does the United States Prevent China from Attacking US Space Capabilities?

Both threats of punishment and efforts to demonstrate US ability to deny military success have problems. Threats of punishment suffer from defects in potency and credibility. Efforts to deny China's success are hindered by US system vulnerability. Both are hampered by US disproportionate dependence on space.

Punishment

It is hard to make threats of punishment sufficiently potent. Tit for tat probably would not work, given greater US dependence on space assets. For example, the threat of retaliating against Chinese reconnaissance or communications satellites if China attacks US space assets could be perfectly acceptable to China. Although Chinese forces are becoming increasingly dependent on space capabilities, even if you project decades into the future, it is unlikely that China will become as dependent on space capabilities as the United States, at least for conflicts in the western Pacific, where China can rely on terrestrial assets for the same purposes for which the United States uses space.

What about going after anti-satellite launchers (with stealth fighters or bombers) if China attacks US satellites? (Some even propose nuclear reprisals, but that is not going to happen.) The problem is that US chances of catching and knocking out mobile anti-satellite launchers are not high, even if it can fly in unopposed. Also, China will likely be launching from western China. Will US political leaders be willing to escalate a localized conflict on the Chinese coast to fight its way in and strike targets deep into Chinese territory and kill Chinese citizens because China attacked an unmanned piece of machinery? For deterrence, can you make these threats credible?

What about threatening the fixed infrastructure that enables tracking and targeting of space systems? Reversible-effects attacks may be conducted using assets that are close to the area of combat. However, the United States will likely have higher-priority targets than, for example, a communications satellite jammer. Attacks on space assets in geosynchronous orbit are likely to be supported by redundant infrastructure spread out across China. Much of the infrastructure for tracking and command and control (C2) is in Chinese cities, including Beijing, which raises proportionality concerns.

When the war escalates to a high level, the threat of punishment becomes largely irrelevant.

Denial

Activities to deny the military effectiveness of attacks fall into the categories of passive and active defenses. Passive defenses are limited and expensive. For example, while the most critical US communications—nuclear C2—are jam resistant, the vast majority are unprotected communications. The trend over the last couple of decades has been to contract out on civilian carriers for communications, but most communications satellite providers do not want to pay for passive defenses.

Active defenses (intercept satellites, escort satellites) have serious challenges in terms of physics, expenses, and capability. Escorting satellites have operational issues—how does an escort satellite actually protect another satellite? Even if it can, an escort satellite is only good for protecting one satellite in one orbit. Moreover, the United States does not even have adequate situational awareness to support passive defenses, which is a less difficult challenge than for active defenses.

Notwithstanding all these challenges, in considering options for active defense, there are missteps that can make the stability problem even worse—such as putting weapons in space. It is questionable how weapons in space would support deterrence given the limitations of what an armed satellite could do to defend other satellites or even itself. Space is an offense-dominant environment—it is easier to attack assets there than to defend them—so stability would be a problem. If the United States put weapons in space, China might do so too; then, in a crisis, each side would have an incentive to shoot first. Finally, violating the taboo about space weaponization that has emerged over the decades would be politically costly for the United States in the international community. Considering all of these factors and the high cost of space lift, the risks and costs of putting weapons in space would almost certainly outweigh any prospective benefits.

Norms

Norms have some effect at low levels of confrontation and conflict, but when push comes to shove and the fighting begins, norms alone will not suffice. However, they have a role in strengthening first-strike stability in space by both reducing benefits and raising costs.

What Does the United States Do?

In developing an answer to this question, start with some basic principles. First, it is important to recognize that it is usually not productive to speak generally about space deterrence. Rather, the United States must identify which kinds of attacks on which portions of which space systems and under which circumstances it is trying to prevent.

Second, the United States cannot deter all kinds of attacks in space. While reversible-effects attacks have so little cost associated with them that they are likely not deterrable, kinetic attacks are a reasonable threshold for general deterrence, at least until the war escalates.

Third, do not think in the stovepipes of space deterrence, nuclear deterrence, cyber deterrence, etc. The Chinese have a more holistic view of deterrence than the United States does. These facets of deterrence are interdependent and should be considered together.

Finally, the United States should stop sending mixed messages to the rest of the world. For example, it says that it does not want to see attacks in space, but in unclassified national space policy and military doctrine, it talks about space control and dominating space in a manner that implies that it thinks fighting in space and warfare in space are acceptable.

With these principles in mind, following are recommendations on space policy, strengthening the credibility of threats of punishment, and increasing US ability to deny benefits.

Space Policy

To strengthen deterrence and first-strike stability, begin with a top-down coherent national space policy. Start with explicitly condemning the use of force in space. Declare that if others attack US space capabilities, the United States will respond in ways, times, and manners of its choosing. Avoid unclassified references to space control and force application missions in space. These policies would reinforce norms against space attack by undermining adversary efforts to depict the United States as seeking to dominate space or develop offensive space capabilities. They would also provide a vague general threat in declaratory policy while shaping the international environment to make specific threats more credible and build international support for carrying them out, if necessary.

Make Threats of Punishment More Credible

As the space warfare taboo strengthens, threats to punish its violation become more credible. Thus, US policy should focus on strengthening the taboo and making punishment for its violation more expected, more acceptable, and more feasible.

Thus, US policies and statements should aim to shape international perceptions by conditioning the international community to accept the justice of the United States punishing aggressors and conditioning potential adversaries to take seriously threats of terrestrial punishment in return for attacks on space systems. In addition, the United States should be willing to engage in "brinkmanship" with adversaries in a crisis. This involves fashioning threats of terrestrial punishment (diplomatic, economic, and military) in ways that put the onus of avoiding catastrophic escalation on the adversary's shoulders. Finally, the United States should develop means of exacting retributive costs on the enemy's space systems. Although tit for tat is unlikely to work to US advantage, enemies must understand that they too will suffer costs in space if they strike first.

Increase Ability to Deny Benefits

This, too, involves managing perceptions. The United States should emphasize the resilience of its orbital infrastructure and alternative capabilities while never divulging specific vulnerabilities. It should make clear to adversaries that, if worse comes to worst, the United States will fight through regardless of what happens to its space infrastructure.

Beyond that, the United States can make its space capabilities more robust over time by investing more in passive defenses; considering subsidizing passive defenses on commercial satellites; continuing research on active defenses to identify technological breakthroughs; dispersing space capabilities across a larger number of platforms (as in GPS) and away from capabilities provided by single, high-value satellites; making satellite manufacture and space lift more responsive to replenish losses more quickly; developing terrestrial backups to space support wherever possible; and exploring stealth, concealment, and deception concepts to complicate the adversary's targeting problem.

Deterring Chinese Space Attacks: Key Questions and Participants' Responses

This section presents participants' perspectives on the agenda questions associated with the workshop session titled "Deterring Chinese Space Attacks." The two sources of information for this section are (1) group discussions conducted immediately after the presentation and (2) computer inputs provided at the end of the session.

Q Can the United States effectively dissuade space attacks without demonstrating willingness to retaliate (i.e., are protection strategies and establishing behavioral norms sufficient for preventing space attacks?)?

There was a broad divergence of opinion on the answer to this question. Respondents were divided among *no*, *yes*, *maybe*, and e*ven retaliation might not be enough*.

Arguments for *no* were:

- No, the United States needs to do both, and, if necessary, it may need to actually retaliate.
- No, because countries will place their perceived interests in a crisis or war as being more important than adhering to a norm of this sort, especially considering that an attack on a satellite would not kill anyone. Moreover, in a high-intensity conflict, it is very much in a US adversary's interest to attack US satellites, and the United States will probably be hitting whichever targets it plans to hit anyway, so US enemies will attack US satellites if they can.

Arguments for *yes* were:

- A modicum of deterrence (even as much as a hint that US behavior would become erratic if it lost the information assurance that space capabilities provide) coupled with a set of alternatives (unmanned aerial vehicles) that substitute for much of the space capability might work.
- Yes, through the ability to impose political costs on core values of the Chinese Communist Party leadership.
- The United States can deter kinetic attacks, and, unlike other domains, international norms may have some impact—there is somewhat of a taboo about space warfare. Moral superiority in any conflict with the United States will be important, and so if countries will really unite and react strongly, it is possible that this will impact the Chinese calculus.

An argument for *maybe* was:

- Possibly, but it would require not only reducing the vulnerability of US space systems and establishing norms but also reducing US reliance on space systems to make such attacks less attractive in the first place.

Finally, several respondents raised the point that even retaliation might not suffice:

- Demonstrating willingness to retaliate might not be enough either, unless the other side is at least somewhere close to as reliant on space systems as the United States.

If they are much less reliant on space than the United States (even if they are roughly equally reliant overall but less so in a particular scenario), they might conclude that the benefits of attacking US space systems would outweigh the costs of whatever damage the United States might inflict on theirs.

- Unless US systems are invulnerable, or unless the United States does not depend on space for military, economic, and other purposes (i.e., space systems are irrelevant), it cannot dissuade space attacks. The ability to retaliate is less relevant. Also, it is *not* clear that China is becoming more dependent on space, or more precisely, that it will become *as* dependent or *comparably* dependent on space as the United States.

A number of respondents emphasized the importance of context for any attack on US space assets, which is likely to involve a broader US–China conflict:

- It is hard to conceive of attacks on space assets occurring outside the context of a broader conflict.
- Behavioral norms will have almost no deterrent effect on China's willingness to launch space attacks. Protection strategies, on the other hand, seem more promising, although attacking space assets will probably always be cheaper and easier than defending them. In other words, deterrence by denial would be great, but it is hard to be optimistic. That leaves deterrence by punishment, which faces its own problems, ranging from a lack of key Chinese space capabilities to difficulty of identifying and hitting comparable targets. On the other hand, if China is attacking US satellites, then the United States is almost certainly already engaged in a full conventional conflict, which means that it is already hitting most strategic targets. So, in the end, it is quite pessimistic to think of the US ability to deter space attacks in scenarios in which the Chinese would actually contemplate doing so.

Q Are there effective retaliatory threats that stay within the space domain, or must retaliatory threats cross domains to be effective?

Asymmetries between the United States and China regarding dependency on space were noted by many respondents, leading to the judgment that effective retaliatory threats must cross domains:

- Asymmetries in how the United States and China define and perceive the space domain are important here. It looks as though the Chinese take a more expansive view of the domain than the United States.

- Given the asymmetries in dependence on space support between the United States and China, it is hard to think of any retaliatory threats that stay within the space domain that would be effective in deterring attacks on US space systems. China's potential future reliance on satellites to locate and target US carrier task forces in the DF-21 era might hold a possibility for holding Chinese reconnaissance and ocean surveillance satellites at risk to deter them from attacking US corresponding assets; however, it is likely that US Navy and Joint commanders will argue that the United States will need to target China's satellites to interdict that kill chain regardless of whether the Chinese exercise initial restraint. With this in mind, it will be difficult, perhaps impossible, for US leaders to make credible assurances of restraint.
- Given asymmetries of dependence, capability, and roles, it is unclear what space retaliatory measures would be.
- Focused on China and on conflicts in the western Pacific, the asymmetries in dependencies in space are so profound that any credible threat the United States could pose in the space domain would be insignificant compared to the cost of the loss of US space assets. The only effective threats would be across domains to find targets of comparable value to hold at risk. The challenge there, of course, is establishing the necessary precondition to an effective deterrent: a clear path of escalation unconditionally set in the mind of the adversary.
- Must be cross-domain. The United States depends more on space than anyone else does, so space versus space retaliation and counter-retaliation hurts it more than them.
- Because of asymmetries, a retaliation strategy (at this point) that does not cross domains is unlikely to be very dissuasive.
- One of the key challenges in cross-domain discussions is the dialogue about the relationships between one domain and all the other domains. In the strategic view, a space attack might require the United States to retaliate in the most appropriate domain. True cross-domain strategic approaches should require the National Command Authority to select the most appropriate domain or combination of domains—with the appropriate proportionate or disproportionate response—to include the timing of the response.
- It likely depends on how dependent the adversary country is on space systems. If it is highly dependent, effective retaliatory threats could be in-kind. If it is much less dependent on space, the retaliatory threats would probably have to cross domains so they could threaten something of greater value to the adversary.

- The United States needs to think harder about the idea of proportionality vis-à-vis Chinese attacks against US space assets. Punishment probably needs to be inflicted on non-space assets.
- I think the answer turns on one's assessment of China's reliance on space assets, in particular, the degree to which it will or will not become more dependent on space systems. The more that China relies on space capabilities of its own, the more effective US retaliatory threats that stay within the space domain will be. Otherwise, cross-domain retaliatory threats seem the only option, even if that remains a poor one.

Q What principles should guide the development of US cross-domain deterrence policies for space (e.g., are red lines useful, and, if so, what should they be and how should they be communicated?)?

Several respondents focused on the potential for, and problems with, red lines:

- The United States probably cannot deter things like dazzling and jamming, but maybe it could establish a red line that prohibits destructive attacks (those that generate debris in space) or a red line that prohibits attacks against certain types of satellites (such as missile early-warning/launch-detection satellites).
- Red lines might make more sense here than in the cyber domain because of the seemingly greater clarity in type and nature of attacks. However, any circumstance where China is conducting anti-satellite attacks will already (or immediately) involve the United States conducting extensive conventional and cyber operations—so the United States will be well beyond cross-domain deterrence and into cross-domain warfighting.
- The United States may be able to deter attacks on its satellites during peacetime/crisis/limited skirmish by stating that it will treat an attack on US satellites as an attack on the US homeland. The United States *cannot* deter attacks on its satellites during high-intensity war unless it is willing to go nuclear.

Other respondents focused on damage-limitation capabilities such as protection, redundancy, and mitigation:

- The United States needs to improve its non-space capabilities for various functions provided by satellites so as to reduce the payoff to an adversary from attacking US space assets. Better non-space capabilities may be the most important single step that the United States could take.

- Space systems are inherently vulnerable in wartime, and the United States does not want to be in a position where it has to escalate beyond standard conventional war to keep enemies from attacking US satellites. A more robust strategy is to replace satellite capabilities with unmanned aerial vehicle and related radio frequency capabilities.
- The United States should emphasize the ability to fight through a counter-space attack, but if the attack in question truly undermines US conventional power, US stakes in the conflict will have dramatically increased.
- There is definitely a need for enhanced resilience and bolstering norms against space attacks.

One respondent emphasized that deterrence relies on identifying and holding at risk assets in other domains that the Chinese value:

- The United States needs to identify Chinese assets that are as important to China as space assets are to the United States (surveillance systems to locate and track US aircraft carriers are one possible example). Holding these assets at risk could form the basis for cross-domain deterrence. However, for such a strategy to be effective, the United States should (1) be able to signal, in a crisis, that it is capable of holding such assets at risk and (2) be willing not to strike these assets if China does not attack space assets.

One respondent focused on the problems of attribution and shared space assets:

- Assigning attribution to acts in space is more difficult than people think. If an attack occurs without the generation of debris (or even if debris is generated), it is often difficult to determine attribution with certainty. The element of deniability makes retaliation more costly in the international community. The best option for the United States is to conduct its own retaliatory attacks quietly, preferably disabling Chinese space (and possibly other) assets without obvious kinetic strikes.

  The problem becomes more complicated because many space assets are shared: what should the reaction be if a commercial satellite is attacked, especially if the attack is reversible and attribution is not certain? The United States should explore policy options that include improving its capabilities to attribute sources of attacks (of all natures: kinetic and non-kinetic) and identify what nations share use of commercial satellites with it (e.g., European Union, Canada, India, etc.).

  Finally, the impact on norms of behavior in conflict that extends to space should be considered beyond simply United States versus China. Russia and emerging space powers such as India (both of which are neighbors to China and are potential adversaries) should be brought into the discussion early. Chinese losses in space would

put them behind their neighbors, and this prospect should deter their willingness to risk losses to space assets at the hands of the United States, especially because their problems with attribution are even more severe.

5

DETERRING CHINESE NUCLEAR USE

While nuclear use by China or the United States against the other may seem far less likely than other threats discussed during this workshop, the physical, social, and psychological consequences of any such use would, in many scenarios, dwarf those due to warfare in other domains. However remote, the possibility of escalation to nuclear war provides a backdrop to even minor confrontations. Also, should a severe crisis emerge, both the United States and China recognize the need to deter nuclear use and counter nuclear threats by the other. At the same time, the United States and China have significantly different policies, strategies, and forces. Lack of appreciation of these differences and the reasons for them can undermine stability by encouraging mirror imaging and other forms of erroneous thinking.

The first section summarizes the presentation on deterring Chinese nuclear use provided at the workshop, followed by key questions and participant responses.

Presentation Summary: Deterring Nuclear Threats in a US–China Crisis or Conflict

by Michael Chase

Sources for this presentation include the following: (1) for force modernization information, unclassified authoritative US intelligence community assessments such as the Department of Defense China military power reports,[15] National Air and Space Intelligence Center ballistic and cruise missile reports,[16] and Office of Naval Intelligence People's Liberation Army Navy reports;[17] and (2) for policy, strategy, and doctrine, Chinese language books such as the *The Science of Strategy*, *SSAC*, and *Intimidation Warfare*; articles from journals such as *China Military Science* and *Military Art*; and selections from *Second Artillery* newspaper and other Chinese military newspapers.

It is important to recognize the limitations of Chinese doctrinal publications. First, although they reveal how China's military *plans* to fight and what the United States should look for in training and exercises, they do not necessarily dictate how it *will* fight. In any severe crisis, nuclear decision making would ultimately fall to a very small number of senior Chinese Communist Party leaders, many of whom probably never thought much about the details of nuclear warfighting. In addition, changes in China's external security environment could erode its traditional logic of minimum deterrence, reducing the relevance of some current writings. For example, while the United States is currently the most important component in Chinese nuclear calculus, certain events could make regional nuclear deterrence rise on China's list of priorities. Significant problems could develop in China's relations with Russia or India, or Pakistani actions might precipitate an Indian response that China views as threatening to its own interests.

Policy

Chinese strategists see nuclear weapons as useful primarily for deterring nuclear attacks or countering nuclear coercion. Thus, China has maintained a No First Use policy since its first nuclear test in October 1964; contemporary Chinese doctrinal publications continue to

[15] US Department of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China* (2013), http://archive.defense.gov/pubs/2013_China_Report_FINAL.pdf.

[16] National Air and Space Intelligence Center, *Ballistic & Cruise Missile Threat*, NASIC-1031-0985-13 (Wright-Patterson Air Force Base, OH: National Air and Space Intelligence Center, 2013), https://www.hsdl.org/?view&did=36478.

[17] Office of Naval Intelligence, *The People's Liberation Army Navy: A Modern Navy with Chinese Characteristics* (Suitland, MD: Office of Naval Intelligence, 2009).

adhere to No First Use. The People's Liberation Army Second Artillery Corps emphasizes survivability of nuclear forces because it is presumed to be extremely likely these forces will be ordered to launch unless they have already been attacked.

The *SSAC* suggests that nuclear deterrence could also counter conventional strikes against strategic targets. Higher-intensity deterrence measures that lower the nuclear threshold could invoke more explicit nuclear threats to ensure that enemies clearly understand the risks they have exposed themselves to or could adjust the No First Use policy by conducting a nuclear demonstration or a smaller-scale nuclear strike. Although it is unclear whether China would launch a nuclear strike in response to a conventional attack, *SSAC* mentions four conditions under which this might happen:

1. When the enemy threatens to launch conventional strikes against China's nuclear facilities or nuclear power stations;
2. When the enemy threatens to attack major strategic targets like hydroelectric power stations (such as Three Gorges);
3. When the enemy threatens to carry out attacks against the capital, major cities, or other political or economic centers; or
4. When China faces impending disaster because it is losing a high-stakes conventional conflict.

Whichever higher-intensity deterrence measures are taken, their purpose would be to frighten the enemy into stopping its conventional attacks or, at least, to reduce the effectiveness of their attacks. Such measures could only be undertaken under the authority of the top-level political leadership of China. There is some discussion in the literature that higher-intensity deterrence actions could trigger escalation, rather than deter it, but not a lot of in-depth discussion of how to avoid this outcome or which factors would hinder or contribute to such an occurrence.

Strategy and Posture

Chinese analysts do not describe their posture in official documents as "minimum deterrence" but rather as "a lean and effective" nuclear force that meets China's national security needs.[18] Contemporary Chinese authors also refer to "minimum," "maximum," and "medium" strength nuclear deterrence. A minimum-strength nuclear deterrent would threaten a handful of secure nuclear retaliatory weapons; a maximum-strength nuclear deterrent characterizes the US–Soviet relationship during the Cold War, involving thousands of nuclear retaliatory weapons. China is transitioning from a minimum-strength toward a medium-strength nuclear

[18] Information Office of the State Council, People's Republic of China, *China's National Defense in 2006*, http://www.fas.org/nuke/guide/china/doctrine/wp2006.html#0.

deterrent, a much more substantial force than it had in the past but still much less than that of Russia or the United States.

Similar to US nuclear strategy, the primary goal of China's nuclear strategy is to "deter other countries from using or threatening to use nuclear weapons against China."[19] Chinese nuclear policy emphasizes "no first use of nuclear weapons at any time and under any circumstances," although exceptions for certain conventional attacks are possible.

China's nuclear force modernization is aimed at creating a "lean and effective" nuclear deterrent that meets China's national security needs. The number of weapons China views as appropriate is driven by evolving Chinese perceptions of its threat environment, including threats to its nuclear deterrent from both conventional and nuclear attacks as well as missile defenses. Also, China does not want an excessive number of nuclear weapons. At best, an excess is a waste of resources; at worst, it could be destabilizing and undermine China's security.

Beijing's current emphasis is on enhancing the survivability and firepower of its nuclear force by deploying road-mobile intercontinental ballistic missiles (ICBMs) and nuclear-powered ballistic missile submarines (SSBNs). To develop these systems, China is pursuing a number of enabling technologies, including warhead miniaturization (for smaller, mobile missiles and MIRVed systems); improved ability to penetrate missile defenses; improved operational command, control, and support systems; and improved accuracy, as well as increasing the number of missiles and warheads. With these new systems, China's nuclear forces will eventually be composed of a road-mobile ICBM (some MIRVed), a silo-based ICBM, and a sea-based strategic deterrent.

China has traditionally maintained its nuclear forces at an extremely low level of readiness. This is likely changing with China's emphasis on survivability and the transition to road-mobile ICBMs and SSBNs. Some units will regularly be at high levels of readiness, while others will not. The Chinese apparently practice moving from one level of readiness to another.

China's emphasis on a secure second-strike capability could contribute to greater stability in the US–China strategic relationship because there would not be an incentive for either side to launch a large-scale strike. As China increases the survivability of its nuclear force, the United States will come to realize that any attempt at a damage-limitation strike would not be in its interest because China will still be able to retaliate with a significant number of nuclear weapons. China will become more of a medium nuclear power, smaller than Russia and the United States but larger than it is today. As such, China could complicate future arms

[19] Ibid.

control negotiations, and aspects of Chinese doctrine could heighten escalation risks in a crisis or conflict.

Nuclear Counterstrike Campaigns

Writings emphasize that any nuclear counterstrike campaign would be strictly controlled by the Supreme Command. It could be conducted solely by the People's Liberation Army Second Artillery Corps or jointly with the People's Liberation Army Navy. The People's Liberation Army Air Force does not have or want a nuclear mission at this time. The objectives of a nuclear counterstrike campaign would be principally aimed at de-escalation or termination of a conflict.

What would China strike? Chinese writings do not discuss striking what the United States would call counterforce targets such as ICBM fields. However, they also do not emphasize pure counter-value (i.e., cities) targeting. They consider a wide range of both military and civilian targets, including military bases and command centers, communications and transportation hubs, political and economic centers, important industrial facilities, and other strategic and campaign-level targets. One change from the past is that there seems to be less discussion about striking concentrations of forces. Older statements were probably based on concerns about massing Soviet troops, but China is no longer as worried about ground invasions.

Chinese writings also do not emphasize electromagnetic pulse (EMP) strikes, but such strikes would be consistent with China's strategic-level political objectives of changing the enemy's decision calculus, in addition to the physical effects of such attacks.

Deterring Chinese Nuclear Threats: Key Questions and Participants' Responses

This section presents participants' perspectives on the agenda questions associated with the workshop session titled "Deterring Chinese Nuclear Use." The two sources of information for this section are (1) group discussions conducted immediately after the briefing and (2) computer inputs provided at the end of the session.

Q Does China share the US goal of isolating the nuclear domain?

Some respondents questioned the premise of this question—that the United States truly has the goal, or takes it seriously in practice—of isolating the nuclear domain:

- Rhetorically, both the United States and China seek to isolate the nuclear domain (China declares no first use; the United States seeks to create the conditions to allow sole purpose). Neither commitment is entirely credible over the long term. At the operational level, neither side isolates the nuclear domain. The United States has dual-use B-2s, B-52s, early-warning, etc. China has shared C2, missiles with conventional and nuclear variants, etc.
- The United States does not explicitly seek to isolate the nuclear domain as a matter of policy, but it has stated that it wants to move toward a policy that de-emphasizes nuclear weapons and relegates them to the sole purpose of deterring nuclear threats; the United States clearly states that it is not there yet. It still considers nuclear weapons a viable deterrent to some types of conventional or other nonnuclear attacks. The United States blurs the line with missile early-warning satellites, B-2s, etc.; China also blurs the line, at least to some extent, with a strategic missile force that fields nuclear and conventional systems. China seeks to mostly isolate the nuclear domain with its No First Use policy but also to deter at least some conventional attacks with strategic effects.

Other respondents were fairly evenly divided between answering in the negative and expressing uncertainty. Those who answered *no* pointed to the role of nuclear weapons in countering US conventional superiority:

- No, it is not in China's interest to share this goal. Its nuclear force represents a strong counter not only to US nuclear intimidation/coercion but also to US advanced conventional weapons.
- No, China does not share the goal of isolating the nuclear domain today, at least not in a high-stakes conventional conflict where China is losing. In such a circumstance, China will see huge incentives to escalate to the use of nuclear weapons to coerce the United States to halt combat operations before China suffers the consequences of conventional defeat. In short, whereas the United States would like to fight and win its wars at the conventional level (because it possesses conventional superiority), China will see nuclear escalation as a tempting strategy for compensating for its conventional weakness in a high-stakes war. The United States may want a clear firebreak, but it faces different strategic circumstances. Rhetorically, China may claim to want to isolate (and eventually eliminate) nuclear weapons, but unless China can reverse its conventional inferiority, there is not much stock in that rhetoric.

The respondents who emphasized uncertainty offered the following points:

- I don't know. Chinese goals can change without notice, depending on the views of the top leadership at any given time.
- I am not at all sure that this is true for China; maybe rhetorically, but not operationally or in practice.

Q What US actions in other domains could provoke Chinese nuclear threats or use?

All respondents mentioned large-scale conventional attacks, especially those threatening Chinese Communist Party legitimacy or China's nuclear deterrent capability:

- Attacks on C4ISR, critical infrastructure, large-scale counter-value attacks (e.g., Tokyo 1945, Taiwanese secession or Tibet, and insurgency support in Xinjiang and Tibet).
- US actions include conventional or possibly cyber attacks against nuclear forces or associated command, control, and communications systems; those that convey the impression the United States seeks to overthrow the Communist Party, kill the party leadership, or otherwise pursue regime change; those leading to a catastrophic military defeat that could gravely imperil domestic stability or could potentially lead to the collapse of the regime; or perhaps more likely, actions that are misinterpreted or misunderstood by the Chinese as being aimed at these objectives or lead to inadvertent escalation through some other type of miscalculation.
- Jeopardizing Chinese Communist Party authority/survival would probably raise questions about nuclear use. This may not be limited to US nuclear use but also US support for other states/entities that jeopardizes Chinese Communist Party authority/survival.
- Large-scale conventional attacks against targets in China, especially targets deep inland or associated with national leadership, could easily cause escalation to the nuclear level.
- US actions could include kinetic attacks against Chinese strategic or leadership targets or possible non-kinetic attacks against nuclear C2.
- Looming Chinese defeat in a high-stakes conventional war could trigger nuclear escalation as a means of coercing a military stalemate that would forestall that outcome.
- Actions include US conventional attacks against Beijing, Chinese nuclear forces, or Chinese nuclear power. Another alternative is a large-scale US conventional defeat of Chinese forces that risks the legitimacy of the Chinese Communist Party.

Q What Chinese actions in other domains could provoke US nuclear threats or use?

Analogous to some answers to the previous question, respondents identified scenarios involving Chinese first nuclear use and impending catastrophic US conventional defeat. Some responses suggest that US concern with the survivability and/or legitimacy of its own leadership is a concern that parallels that of the Chinese Communist Party:

- Same as the previous question, and also consider similar attacks on these targets of US allies. For all these questions, there are the risks of unintended or unforeseen consequences, miscalculation, inadvertent escalation, and the fog of war that must be reckoned with.
- Potential Chinese actions include those that lead to a catastrophic or humiliating defeat that could shatter US credibility, gravely undermine US alliances, and severely diminish US regional influence and interests—or perhaps more likely, actions that are misinterpreted or misunderstood as being aimed at these objectives or that lead to inadvertent escalation through some other type of miscalculation.
- Chinese actions that precipitated massive US casualties or existential survival questions would provoke US nuclear threats. Chinese use of nuclear weapons would precipitate US nuclear threats/use.
- What impact would sinking a US carrier battle group have?
- The Defense Science Board suggests a sufficiently severe, high-casualty event might instigate the United States. Overrunning a US ally (e.g., Republic of Korea) might also have the same effect.
- Other actions include large-scale Chinese conventional defeat of US forces (e.g., multiple carriers sunk).
- Any action that would result in damage and casualties on par with a nuclear attack could provoke a US nuclear threat or use.

Some respondents did not believe there were plausible scenarios in which the Chinese could provoke US nuclear use:

- There are not any foreseeable, plausible Chinese actions in the nonnuclear domain that would provoke US nuclear threats or use.
- It is hard to see how any credible Chinese conventional/cyber attacks would be an existential threat to the United States, so it is unlikely that the United States would go nuclear. Moreover, China is unlikely to pursue any strategy aimed at inflicting

huge civilian casualties or massive damage to US infrastructure through the use of conventional weapons. The United States will not use nuclear weapons to keep China from conquering Taiwan, and it may not even be willing to conduct large-scale conventional strikes against targets in China.

- This is not likely. The United States has a strong sense of the nuclear taboo, and since the end of the Cold War, it is not apparent that use of nuclear weapons is part of national strategy.

Q Do Chinese authors predict that their own or US precision conventional, cyber, or space attacks will elicit a nuclear response?

This question differs from the previous two questions in that it focuses on Chinese writings. Respondents indicated significant uncertainty in their answers:

- In some cases, yes, depending on the author involved and the targets attacked by the United States. It is unseen whether they predict US nuclear response in public, though one obviously cannot be sure in private.
- People's Liberation Army writings indicate that combined deterrence is likely to lead to deterrence of US nuclear use. It is unclear what would elicit a nuclear response.
- It is not likely. China very rarely considers and accurately determines how its actions are interpreted by others. It views its actions as defensive and therefore not provocative.

Q Should the United States explicitly retain or relinquish the option to respond to cyber and space attacks with nuclear weapons, cultivate ambiguity, or be silent on the matter?

Almost all respondents opted for ambiguity or silence, some noting that silence will foster ambiguity:

- The United States should cultivate ambiguity to make China see that it is potentially playing with real fire.
- Silence is golden. It breeds ambiguity.
- The United States should be silent about possibilities of responding to cyber or space attacks with nuclear weapons. It should not make any explicit threats that lack credibility, and it is inconceivable that the United States could convince anyone that it would resort to nuclear weapons against any state, much less a nuclear-armed adversary, in reprisal for attacks on uninhabited machines in space or US computer networks. The

only way such attacks could lead to a US nuclear response would be if they degraded US warfighting capability so severely that the United States was on the verge of an unacceptably catastrophic military defeat (whatever that might be). However, even in those circumstances, it would be events in the terrestrial domain that would lead to the risk of nuclear escalation, not the space or cyber attacks in isolation. Therefore, threatening a nuclear response in efforts to deter space and cyber attacks would not be credible.

- Be silent on the matter. Making threats that the United States cannot make credible only propagates the impression of US fear of such attacks, potentially increasing the probability an opponent would carry them out. Silence will result in ambiguity.
- The United States should cultivate ambiguity or be silent on the matter, but if this is about rhetorical policy, then this issue does not matter much.

One respondent suggested relinquishing the option to respond to space and cyber attacks with nuclear weapons:

- Everything depends on whether it is US policy to reduce the number of situations/contexts in which nuclear use is contemplated. If so, the answer is to relinquish the option because any cyber attack implicates the systems' owners as well as the attacker, and there are no space assets that could not be replaced within a few years.

6

FUTURE RESEARCH

In the final workshop session, three questions were posed with the intention of identifying future research needs and productive research approaches. Each participant was asked to verbally address one (or more) of these questions and to provide any additional input using the computer.

Q What else does the United States need to understand about China?

Several respondents focused on understanding central aspects of China's strategic culture—its role in the international system, its values, and its fears:

- The United States needs to understand that China sees itself as a status quo power and how it defines and defends the status quo as it sees it. Both the United States and China may see themselves protecting the status quo but find the other's actions as offensive. History shows that wars are not caused by rising powers threatening international systems but by declining powers unwilling to relinquish their positions gracefully.
- The United States needs a better sense of what the Chinese Communist Party values because deterrence can succeed only when it can hold at risk what China values. The United States assumes it is China's nuclear capabilities and thinks it might be China's economic advances. The United States canonically assumes population is most important, but maybe it is not. It emphasizes the Chinese Communist Party survival/hold on power. However, how does one go about threatening that? Defeating them in war? Eliminating the People's Armed Police (PAP) database? Destroying cities? Propaganda?
- At levels of violence lower than holding at risk the Chinese Communist Party's grip on power, the United States needs to identify China's fears. What assets does China most fear the United States will hold at risk in a crisis (equivalent to US concerns about its space assets)? If those fears are known, then the United States can take advantage of them and enhance deterrence.

Other respondents focused more directly on deterrence and compellence:

- The United States needs to understand everything about China's approach to nuclear warfare and deterrence from its reference point, rather than in the context of US deterrence theory. Mirror imaging must be eliminated. The United States and China do not think of deterrence in the same way. The United States must not presume that China thinks about strategy, politics, escalation, and information warfare and operation the way the United States does.
- The United States needs to better understand deterrence of the strong by the weak. This requires a much more rigorous examination of the use of nuclear weapons to deter conventionally superior adversaries, whether locally or globally.
- The United States needs to separate peacetime deterrence of the use of force and deterring further escalation during wartime or limited conflict. How does China see

these differences? What happens when you move beyond Phase 0 or Phase 1 and need, in a limited war, to deter hostilities from moving into other domains? Under what conditions would China capitulate rather than escalate? There is a huge divergence in opinions among people with different backgrounds on the question of how you would persuade the Chinese to decide to discuss, rather than escalate, the conflict.

- Deterrence involves taking a course of action to dissuade China from action. The flip side of this is coercive persuasion: how to persuade China to act as you want it to act. Objectives of coercive persuasion might include stopping intrusive cyber surveillance and stealing intellectual property; adopting a much more conciliatory policy about the territorial claims in the South China Sea or East China Sea; and accepting the reality of Taiwan's existence as an independent sovereign state within a One-China framework. How does China conduct coercive persuasion?

Q Are there specific scenarios that should be examined?

Tabletop exercises provide a primary analysis tool to explore strategy, options, crisis evolution, and decision making. However, such exercises are only as good as the scenarios on which they are based. We have therefore posed this question to the workshop to help shape an effective agenda for research.

There was no shortage of participant suggestions regarding scenarios. Many suggestions involve combinations of actors other than a direct confrontation between the United States and China. Such scenarios included those in which the United States is not a principal actor; others involved China and a US ally or China and another regional actor; and still others involved neither the United States nor China as the principal actors:

- With respect to scenarios, discussions so far have pitched the United States against China building to, or in, some type of conflict. A more plausible scenario may be one in which China has an altercation with an ally of the United States, with the United States acting as a third party. As the altercation escalates, what role should the United States take in deterring both parties from further escalation?
- China–India, China–Vietnam, and China–Russia are scenarios that must be examined, not just Taiwan or Japan, and we have not considered them.
- The United States needs to address scenarios in which China is not one of the main antagonists but could be brought in anyway due to Chinese equities; India–Pakistan or US–Pakistan would be the more interesting of these.

- The United States should consider scenarios in which US allies use or threaten to use their own military capabilities.
- Consider scenarios in which there are many players. Consider scenarios in which other actors take the lead (e.g., India, Pakistan, North Korea, or Taiwan) with a more nationalistic and/or more provocative government.
- The United States needs to play multi-actor scenarios.
- Mostly we address a direct Chinese attack on a US ally. Consider scenarios such as India–Pakistan, in which China is dragged into a crisis with someone else in the region (not the usual direct attack by China on an ally).
- Consider scenarios in which players other than the United States and China, even impoverished states, have significant cyber capabilities. Such a cyber-capable third party (e.g., North Korea) may have caused an attack or at least the evidence suggests so. How would that play out in US–China relations?
- What would happen in a Korean collapse or Korean war?

Three respondents suggested scenarios in which the internal situation in China is an important driver:

- The United States should think about scenarios in which China is not a rising power but is either stagnant or declining. This could be due to a confluence of a number of its various problems (economic, environmental, demographic, etc.). China could see its window of opportunity closing to resolve in its favor some of its outstanding territorial disputes, such as Taiwan. This situation could motivate greater Chinese reliance on nuclear weapons.
- The United States needs to play China with internal dissent and instability and examine how that affects the deterrence equation and escalation dynamics.
- What if the Chinese decision-making structure breaks down, where the Central Committee is no longer in complete control over the forces that are acting?

Two respondents made suggestions on more realistically representing Chinese doctrine and decision making:

- In most war games, Blue (the United States) has all the bureaucratic problems of reality. By contrast, although Red (China) is at least as bureaucratized as Blue, Red is usually played as without any bureaucratic, internal political divides. Thus, the United States needs to play China with a bifurcated command structure, a bureaucratized government, provincial authorities' inputs, and concern for domestic popular opinion.

- Play a series of interactive scenarios, doctrinally informed on both sides. This could help us answer the question about whether doctrine matters at all.

Two respondents suggested scenarios involving a cyber attack that cause unintended yet significant change:

- Consider a significant cyber attack on civil infrastructures in the United States that leads to widespread civil damage but limited direct human casualties. The damages caused by such an attack could have been inadvertent. What kind of response would such an event provoke? How would the United States react?
- What happens when there is a cyber attack that inadvertently causes catastrophic damage (e.g., one that blacks out half of China or causes a catastrophic reaction at a nuclear power plant)?

Two respondents focused on developing and assessing options for responding in various circumstances:

- Consider a crisis with China in which some non-kinetic satellite attacks occur. How does the United States respond to best achieve its objectives? This is an important part of deterrence that the United States is not exploring as much as it should be. Deterrence is too divorced and too separated from crisis response and warfighting.

  It might also want to engage Chinese analysts in a discussion to examine scenarios in which, for example, a natural disaster in space occurs or a cyber attack on critical infrastructure in the United States or Europe, focusing on how the United States and China communicate to ensure stability during the period of uncertainty as to what happened and avoid inadvertent escalation. This approach would allow discussions with China, which is unwilling to talk about these issues in an international US–China context.
- The United States needs to examine a range of difficult scenarios involving cross-domain attacks, in part to develop credible military and diplomatic options to draw from in a real crisis. As an example, consider a crisis that has not escalated, but China starts blinding and jamming US satellites. What do we do? Credible deterrence must be anchored in credible plans and capabilities.

Two respondents suggested scenarios that explore the reaction to nuclear use:

- It seems that thinking stops as soon as there is a nuclear detonation. What happens after a nuclear detonation occurs? The United States needs to discuss ways to de-escalate the situation after the detonation of a nuclear weapon, for example, near a carrier battle group or at a military facility.

- What if North Korea used nuclear weapons? If North Korea killed a million people, the United States would be unlikely to settle for anything less than a regime change. How would China react?

  China has been generally cautious, probably believing time is on its side if nothing throws a monkey wrench into the works. China's GDP is growing fast, as is its standard of living. The economic situation in China is improving compared to other countries, even if it is not yet where it wants to be. Thus, China does not want such a crisis but could be unwillingly involved in a conflict started by North Korea or involving India–Pakistan.

The remaining suggestions do not lend themselves to grouping, other than to note that many are among the least well-examined possibilities:

- Consider lower-end scenarios in which there is coercive persuasion but not enough use of force to ensure a military response with the potential of the situation escalating to military conflict. It is easy enough to envision this for a China–Japan crisis. Also South China Sea scenarios in earlier phases could escalate from Chinese use of economic pressure and maritime law enforcement capabilities (e.g., against the Philippines) to a level at which China might contemplate using military force. Nuclear deterrence would not be relevant at that point; what kinds of conventional, cyber, and space actions or activities could result?
- Consider situations that occur in locations more geographically distant from China that would force the Chinese into greater (than the East China Seas or a Taiwan scenario) reliance on space systems, which could at least partially change some of the dynamics. The stakes would not be as high, nor would conflict be at the same level.
- The United States could also explore scenarios involving China that do not arise out of a conflict. For example, how do the United States and China maintain stability after a natural disaster in space degrades some satellites? The United States has not considered how civilian leaders will think about these catastrophes in a crisis. Do they understand cross-domain relationships, and how might their perceptions differ from the military? Civilian Chinese leaders may be more concerned about economic interests in space than military leaders, who may be more concerned with tactical advantages that stem from less military dependence on space assets.
- The conventional wisdom that disparity in nuclear capability does not matter much in a crisis has not been adequately challenged. Thus, the United States needs to analyze scenarios that explore the importance (or not) of parity in nuclear capabilities. Unfortunately, because it is mainly those who subscribe to the conventional wisdom that would play out the scenarios, it is likely to reflect this conventional wisdom in

scenario-based exercises. We have to think of ways to reduce the likelihood of this happening.

Q What has not been considered?

A number of responses to this question echoed scenario suggestions for the previous question.

- The United States needs to consider options to become less dependent on space. In particular, it needs some form of survivable penetrating ISR to reduce pressure on the satellites. For example, we used to have options for ISR like the SR-71. Aircraft have the advantage of flying unpredictable routes.
- The United States needs further discussions of missile defenses and air defenses. Do these matter? The Chinese are definitely interested in air defense and seem to be interested in missile defense.
- The United States needs to consider how it makes credible assurances to its adversaries (a critical hard issue).
- The United States assumes, perhaps, that it can deter the adversary by structuring threats and posturing forces in certain ways and that it can manage escalation risks in certain ways, ignoring the fact that other actors may be also contributing to the situation. However, it may not be able to constrain or restrain US friends and allies, who feel threatened and have greater stakes in the region, even if they notify us in advance.

  The United States will need to reassure them that it can take on the deterrence and escalation management burdens to protect them. It will need to establish the credibility of its resolve, even in the face of nuclear weapons. It may need to structure deterrent threats against its allies that will restrain them from taking actions that would critically destabilize the situation in a confrontation.
- The United States needs more discussion of credible military and diplomatic response options that might actually be used in a crisis. This is intellectual homework for thinking about deterrence. One of the best approaches is through scenario analysis, some of which presumably is conducted at the classified level.
- The United States should address cross-domain deterrence challenges by using rational strategic logic. Think about these challenges as if the United States faced an anonymous adversary. How would the United States deter actions in domain A by threatening actions in domain B? To address this challenge, it needs to answer the following questions:

(1) What is the strategic context?; (2) What would be in US interests?; (3) What would make a threat credible or not credible? Rhetorical policy is less relevant, and international norms will not matter much once the shooting starts.

- How do you deter a failing state or a desperate state? This question has been insufficiently examined.
- The United States needs to understand the interplay of domestic and foreign imperatives. The biggest threat to China is internal. However, does China really fear existential foreign threats or rather those foreign threats that, in combination with domestic instability, can become existential threats? The Chinese Communist Party might not be able to easily control the domestic situation but could have an impact on deterring the external threat using its nuclear and conventional military forces.
- The United States needs to understand China's perspective on multiple deterrence. What if Russia is not working with the United States, but after China has deployed nuclear weapons at the United States, does it have to worry about having enough weapons left over to deter or attack Russia and possibly other states? How does China view a multipolar world of multipolar deterrence?

7

FINAL THOUGHTS

Cross-domain deterrence, in reality, represents new terminology and new applications of a concept that is as old as nuclear deterrence itself. After all, the first application of deterrence in the Cold War was to prevent Soviet *conventional* attacks against Western Europe by invoking the fear of *nuclear* response. This suggests that, by looking at the historical applications of deterrence in those situations in which multiple domains were in play, analysts could develop lessons applicable to emerging threats and future scenarios.

We also are taken by the diversity of answers to most questions. Clarity and consensus on many cross-domain issues clearly elude the US strategic community. It is unclear how to overcome this or whether it is even possible to do so. Therefore, in addition to historical analysis, it appears that we might also learn from other states' perspectives and policies regarding deterrence, cross-domain and otherwise. Thus, a second potentially fruitful research path would involve comparative analysis of various states' thinking on these questions.

Notwithstanding the general lack of consensus, there was *some* agreement worth noting. For example, few argued against the notion that there is little likelihood of a Chinese attack against US space assets outside the context of a broader conflict.

While we do not take issue with this judgment, we are not confident in it to the point of completely excluding from US planning the possibility of a Chinese surprise attack on US space assets. In fact, there is a perverse dynamic at work here: those contingencies that we do plan for decrease in likelihood because of our planning, while those we do not plan for

increase in likelihood because of our failure to plan for them. This suggests a careful scrutiny of assumptions, explicit and implicit, in cross-domain deterrence analysis.

Finally, this workshop was conducted at what can be characterized as a conceptual level. However, it became clear that considering cross-domain issues at an abstract level is limiting, as almost all cross-domain deterrence decisions are context dependent. Thus, scenario analysis must be an integral component of future research. Moreover, as several participants have noted, scenario analysis could greatly benefit from the analysts trying to emulate Chinese thinking.

As with many workshops, this one has raised more questions than it has answered. We hope that this compilation of the perspectives expressed over the course of this JHU/APL Cross-Domain Deterrence Workshop will provide a useful point of departure for other researchers as they pursue these important questions.

JOHNS HOPKINS
APPLIED PHYSICS LABORATORY