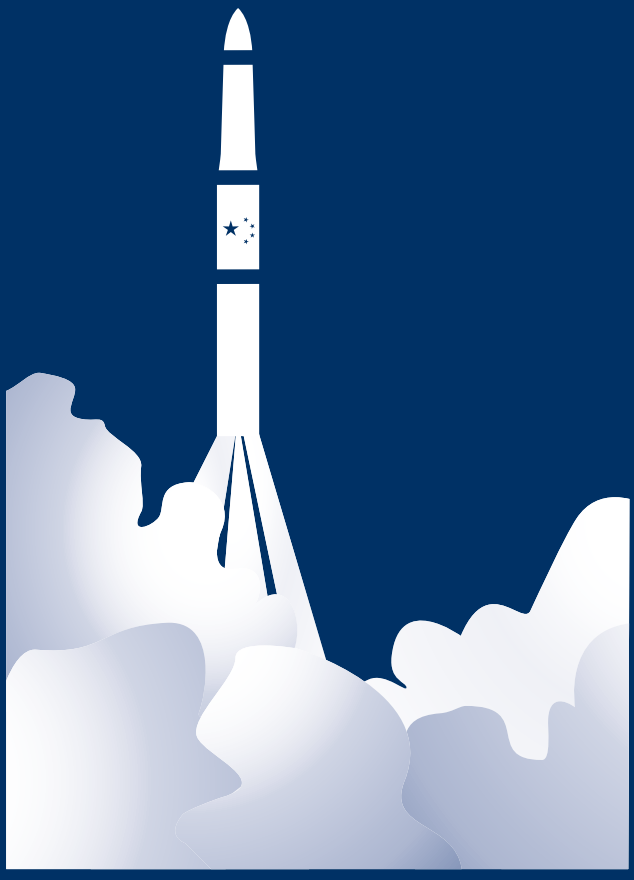


CRISIS STABILITY IN SPACE

CHINA AND OTHER CHALLENGES

Bruce W. MacDonald
With ADM Dennis Blair (USN, Ret.), Dean Cheng,
Karl Mueller, and Victoria Samson

FOREIGN POLICY INSTITUTE
STUDIES IN POLICY

Print Report Design: www.SchumannStudioCreative.com
Printed on Rolland Hitech - with a minimum of 30% post-consumer fiber, made using renewable biogas energy.

For electronic copies of this report, visit:
www.fpi.sais-jhu.edu

The Foreign Policy Institute
The Paul H. Nitze School of Advanced International Studies
Johns Hopkins University
Rome Building, Suite 734
1619 Massachusetts Avenue, N.W.
Washington, D.C. 20036
Tel: +1 202 663 5772
www.fpi.sais-jhu.edu
@FPI_SAIS

CRISIS STABILITY IN SPACE

CHINA AND OTHER CHALLENGES

Bruce W. MacDonald
With ADM Dennis Blair (USN, Ret.), Dean Cheng, Karl Mueller, and Victoria Samson

FOREIGN POLICY INSTITUTE
STUDIES IN POLICY

TABLE OF CONTENTS

ACKNOWLEDGMENTS

With support from the Naval Postgraduate School's Project on Advanced Systems and Concepts for Countering Weapons of Mass Destruction (PASCC), the United States Institute of Peace (USIP) conducted the study "Crisis Stability in Space: China and Other Challenges" from 2013 to 2015, under Bruce MacDonald's leadership. This report, in summarizing the extensive work undertaken, identifies the space security challenges that confront the United States today; reviews the dynamics of crisis stability in space; illuminates some of the dimensions of the strategic landscape of space; and identifies factors that would likely influence space domain behavior in a crisis or actual conflict, with special emphasis on the challenges posed by China, which is currently the United States' biggest potential space adversary. Of particular interest are behaviors that enhance or detract from stability in space. Several elements of cyberspace are also addressed, in keeping with the cyber domain's growing importance and its rising level of interaction with the space domain. While this report's focus is the security interests of the United States, the author hopes this assessment will also be useful to other countries, including China. Security in space, and in other domains, is not a zero-sum game. A better understanding of the space domain's strategic landscape and properties, coupled with wise leadership, can help all countries to harvest the many economic, scientific, and security benefits that space can provide while minimizing the chances for conflict in space.

Drawing on extensive interviews, analysis, and a November 2013 workshop held at USIP to examine the subject, this report seeks to increase the understanding of crisis stability in space and how it functions, with an eye to benefiting U.S. decision-making in day-to-day space operations, in crisis preparedness activities, and particularly in prospective crises and early-stage conflicts. While this report only scratches the surface of these complex issues, it attempts to help the reader grasp some of the mechanisms and characteristics that affect crisis stability in space while contextualizing some of the security challenges that await the world in this domain. Implicit throughout the discussion is an emphasis on the important military role that space will continue to play in the years ahead.

Essential to understanding crisis stability in the space domain is a focus on what factors appear to strengthen or weaken space deterrence and on how deterrence ultimately functions or fails in a crisis. Greater awareness of the space domain's interactions with the cyber and conventional domains, and even with the nuclear domain, would enhance understanding of how to best maintain space stability in a crisis or restore space stability should conflict break out. It also could help the United States to build upon current its space policy and strategy by informing its peacetime decision-making on space behavior, space acquisition, and strategic war-gaming. At this early stage in developing stability concepts for space (and cyberspace), this report draws in part from stability concepts from the conventional and nuclear domains. In doing so, it necessarily raises far more questions than it answers.

I am grateful for PASCC's support of this project, and wish to acknowledge and thank all the people who have directly and indirectly been so generous with their time and insights in conducting this research. I thank USIP and the direct contributors to this report—Admiral Dennis Blair, Dean Cheng, Karl Mueller, and Victoria Samson—for their collegiality and their insightful contributions, which appear later in this report. I also thank Winnie Tsang for providing excellent research support while she finished her graduate studies during the first part of this study. I am grateful to the many, many people both inside and outside of government who generously shared their time to strengthen my understanding of space crisis stability and of other military and commercial space issues. Any mistakes contained in this report are mine, not theirs.

I am also grateful to the Foreign Policy Institute of the Johns Hopkins University's School of Advanced International Studies for their support in publishing this study. Particular thanks go to its director, Carla Freeman, for her encouragement and inspiring collegiality. I also want to express my admiration for Diane Barnes, who edited the drafts of this report with unparalleled skill and diplomacy.

EXECUTIVE SUMMARY

Overview

Information is the lifeblood of U.S. military strength, making the space assets that transmit this information to distant forces extraordinarily appealing targets—especially when those targets are vulnerable. Space has become a critical component of U.S. security, chiefly through satellites that generate and transmit vital information that dramatically increases the effectiveness of U.S. weaponry and military decision-making. The U.S. economy depends on space information as well. In a crisis, the United States and a space-capable potential adversary such as China would likely face an unstable, high-stakes environment that is neither familiar nor well understood.

Understanding space in the context of crisis stability requires grasping its strategic landscape, including how deterrence functions or fails in a crisis and what factors strengthen or weaken that deterrence. Interdependencies between space and other domains are enormously complicated, and their exploration is essential to understanding twenty-first century strategic crisis dynamics.

Space asset vulnerabilities provide an adversary with dangerously attractive incentives to pre-emptively attack in a crisis. In such a scenario, each side would confront the choice of striking first with all its assets in place, knowing that a conflict is beginning; or ceding the initiative, absorbing a first strike, and making a ragged retaliation against an opponent fully expecting such a response.

In "Space and the Evolving Chinese Military," Dean Cheng identifies how China's People's Liberation Army (PLA) sees the ability to exploit information as a potentially decisive factor in future conflicts. This stance prioritizes the development of superior abilities to exploit information in battle while disrupting similar utilization by potential adversaries such as the United States. National economic development is China's top priority, but this objective can only be pursued on a strong foundation of security. Chinese leaders' explicit enumeration of establishing space dominance as a PLA mission reflects the importance of space in its national security. The PLA considers space

to play an important role in the rapid collection, accumulation, and transmission of information, which are all essential tasks in military operations and other areas such as economic development and social stability. China's military emphasizes the importance of planning "key point strikes," which typically include an opponent's command, control, and communications network and intelligence (C3I) infrastructure, including reconnaissance and surveillance systems, where space plays an important role. In one PLA view, "space dominance will be a vital factor . . . [and] directly affect the outcome of wars."

The PLA recognizes U.S. space vulnerability, has written extensively about it, and has tested anti-satellite (ASAT) weapons as part of its broader strategy of winning "informationized" conflicts. The PLA sees space and cyber capabilities as highly important to deterring and, should deterrence fail, defeating the United States through attacks on its most vulnerable and essential elements of military power, which currently are in the space and cyber domains. Until these U.S. vulnerabilities are corrected, our susceptible space architecture will force the United States confront potentially dangerous choices in the space domain. The PLA's goal in space conflict would likely be to fight quick wars with quick resolutions, giving it major incentives to strike first when conflict seems inevitable.

Issues in Space Crisis Stability

The current fundamental challenge to crisis stability in space is the ease and preferability of launching a disabling first strike against an adversary's space assets relative to retaliating against those of an aggressor. This is the essence of crisis instability, where pre-emption pays far greater benefits than retaliation. The weaker or more disadvantaged country in a crisis may find this line of thinking irresistible, or at least preferable to the alternatives.

Another crisis stability threat is the inexperience that nations share in the space and cyber domains, unlike in conventional domains of conflict and in the nuclear domain to a lesser extent. This inexperience gives rise to a "sorcerer's apprentice" problem, placing leaders at risk of making potentially unwise judgment calls without a full grasp of their implications. The space and cyber domains are sufficiently new and dynamic that such decisions are highly likely.

Adding to this uncertainty is the ever-growing interdependence of infrastructures within and among advanced countries, making the impact of major attacks against a country's space and/or cyber infrastructures inherently unknowable. The unpredictable,

cascading collateral effects that could result from a space or cyber attack appear somewhat analogous to the potential use of virulent bioweapons against an adversary; either could cause far more damage than intended, potentially even afflicting the attacking country as much as the one attacked.

Another dimension of the problem is the issue of scale. While jamming one or two satellites in isolation appears unlikely to quickly escalate into all-out space war (given the longstanding role of electronic warfare in past conflicts), attacking multiple intelligence-gathering satellites would carry a far higher risk of escalation. Somewhere between these two extremes, however, is an uncertain and unknowable boundary that divides offensive space actions that modestly threaten stability from those that are clearly destabilizing and escalatory. In this unpredictable environment, a country with no desire to spark an all-out space war may still prompt rapid escalation with modest offensive actions that inadvertently cross an unknown threshold. In addition, the space and cyber domains are evolving far more rapidly than the conventional and nuclear domains, potentially rendering space and cyber strategies ineffective or irrelevant within a few years. In both space and cyberspace, we may learn firsthand how much escalation is too much only after it is too late to stop. Evolving space dynamics could undermine whatever current understanding we may have of crisis and strategic stability in space, and this imperfect grasp of general principles can only add to our uncertainty about the space and cyber offensive capabilities of particular adversaries. Therefore, uncertainty, bluffs, and worst-case thinking are bound to remain prominent forces in the strategic landscape of space.

One bright spot for the United States is its many treaty-committed allies, which would greatly complicate any planning for substantial space offense by China (which has no comparable state partners). Due to the United States' high level of dependence on non-U.S. commercial space infrastructure, a Chinese attack would necessarily extend to additional countries that may otherwise facilitate a U.S. counterstrike, threatening a much wider conflict than China might want to risk.

Space Offense

The impact of space offense on escalation depends on factors such as the nature of the targets hit, whether damage is temporary or permanent, the availability of backups for the systems struck, and what options are available in other domains. What is important is not the space assets themselves, but rather the capability they provide. If the United States can field more survivable space assets, both in orbit and on the earth, a potential space offense would appear less threatening than it does to today's

more vulnerable U.S. space architecture. Similarly, a survivable space offense capability is more stabilizing than a vulnerable one. Space-based offenses appear to be inherently less survivable, and thus more destabilizing, than ground-based offenses. If China and the United States each developed a major offensive space capability, the nation with a more survivable capability would enjoy a major advantage. However, that country would still face an inherently unstable environment where its adversary, in a crisis, would have a huge incentive to strike first in order to avoid losing its vulnerable offensive space assets. Countries sometimes go to war not because they want to, but because doing so appears less risky than not doing so. Any space power would want to avoid being in an unstable use-or-lose situation.

If at least some offensive U.S. space capability is deemed useful, it would be desirable for this system to be:

- Largely survivable against an adversary first strike
- Capable of delivering temporary and reversible effects
- Effective at delivering these effects, with little or no collateral damage
- Survivable
- Resilient
- Little or no collateral damage from offense effects
- Seamlessly connected with conventional, cyber, and other military capabilities
- Flexible, capable of functioning under a variety of scenarios
- Perceived as credible, both to potential adversaries and allies
- Able to maximize adversary risk aversion through minimum susceptibility to countermeasures, sustained capability, and other features

It should be noted that many of these characteristics are relevant to cyber offense as well, whether for space or other applications.

Comparing Strategic Domains

The table on page 44 compares the conventional, nuclear, space, and cyber domains according to 15 criteria, showing that the domains are neither identical nor fully dissimilar. While the space and cyber domains show the most similarity, their characteristics do not come close to fully overlapping. They both change over time far faster than the conventional and nuclear domains, both are enmeshed much more deeply with each other and the world's civilian economy, both have more difficult attack damage assessment, both offer limited conflict experience, and most troubling, both provide major incentives in their current architectures and weapons to strike first in a serious crisis. This implies not only a high level of crisis instability, but also a high potential for rapid escalation.

Discussions with Chinese experts suggest that both China and the United States have space deterrence strategies, but each side suspects the other has a war-fighting strategy for space. The United States may not need space weapons at present to deter China and other adversaries in space, if it is perceived as willing to respond decisively in other domains to potential space attacks. The future is far more uncertain, though, making some level of explicit U.S. space offensive capability appear desirable to avoid granting China a "free ride" in the space domain.

Perspectives on Space Offense, Defense, and Crisis Stability

In his discussion, Karl Mueller offers six important interrelated perspectives on crisis stability in space:

- Events in space do not happen in isolation. Any space conflict would likely be part of a multidimensional game board as are prospective conflicts in other domains, with cyberspace as a possible exception. Space is important because of the effects it has on the earth. Significant instability in space is unlikely to lead to war if there is great stability in other domains and in the larger geopolitical relationship between participants, while conflict could easily spread to a stable space domain if war in other domains appeared preferable to the alternative.

- Incentives for pre-emption and prevention in space are central concerns. If conflict seems unavoidable, even a weaker country might conclude that striking first is preferable to striking second.

- The escalation relationship between space and terrestrial conflict is unclear. The cost of deterrence failure in space may be lower than failure in other

domains—certainly in the nuclear domain—and it would involve less direct bloodshed. The advantages of pre-emption in space, coupled with fewer direct human casualties, could give a space power little reason to exercise restraint in space.

- Offense and defense are viewed differently in space. Space is not territorially divisible; attacking an enemy satellite over one's own country is considered offensive, unlike attacking an enemy aircraft over one's own country. Conversely, defending one's own satellite over another country is considered defensive.

- Space is offense-dominant at the tactical level. Satellites have no terrain to hide behind, are easy to see, and have little capability to maneuver, resulting in significant advantages to striking first.

- At the strategic level, offense-defense dominance in space is more contingent on outside factors.

Different space capabilities have different effects on stability, which would themselves vary in accordance with the participants, location, and stakes of a crisis. The vulnerability of a potentially targetable satellite is not the issue; rather, it is the extent to which the satellite's user depends on information it provides. Space systems generally are more important for projecting military power over long distances than for defending one's homeland, as long-distance contact with forces depends much more on satellites than local operations.

The very novelty of the space, and related cyber, domains may provide seeds for a tenuous stability. The lack of major combat experience in either domain, coupled with the unpredictability of the effects of major attacks in these new domains, may lead to substantial risk aversion among civilian leaders. Leaders could be cautious in escalating beyond modest tactical applications of offensive weapons in these domains for fear of setting off a rapidly accelerating escalation that could engulf the non-nuclear domains in serious destruction and loss of life while threatening ultimately to spread to the nuclear domain. Furthermore, leaders may fear that their own weapons may not be as effective as advertised, and that adversary offense may be more effective than estimated, creating an island of stability where both sides are risk averse.

Given the importance of space to their national security, both China and the United States would probably like to shape the space domain to their own advantage, in ways

that are stabilizing and that enhance their security interests. Attaining such parochial stability would be very difficult for either country, and sustaining it probably more so. China would strongly resist any U.S. attempt to achieve and sustain such dominance, just as the United States would resist a comparable Chinese attempt. A more feasible objective for the United States (or China) would be to make its space architecture less vulnerable and more resilient to attack. A more survivable and resilient architecture would both reduce U.S. incentives to initiate counter-space activity by countering the "use-or-lose" pressures of vulnerable assets while assuring that the military benefits of space would remain available. Failure to solve the resilience challenge could force the United States to escalate quickly in space during a crisis. Such escalation could easily begin from even a modest use of space offense. Without resilience, space adversaries will have major incentives to degrade or destroy the other adversary's offensive space capability, and likely the sooner the better. Cyber weapons may play a role in this process, which themselves will tend to be used early and intensively after conflict breaks out and not spread out over an extended period of time.

In a crisis, the less offensively capable party in space ironically could feel greater pressure than the stronger power to initiate offensive space actions and then escalate quickly. In doing so, the weaker power could both prevent the stronger power from escalating first and avert any additional risk from a more gradual escalation. Under these circumstances, diplomacy would have little chance to avert conflict.

These realities would make space-oriented decisions especially challenging in a crisis, given the worst-case thinking that would likely be present on both sides. Prudent and purely defensive actions such as deployment of backup satellites could easily be misinterpreted as preparation for war. Rendezvous and proximity operations on satellites will become more common in the years to come, but they may be viewed in a crisis as potentially hostile acts. Crisis signaling in space can be useful, but it must be considered carefully due to the potential danger of misinterpreted signals.

Future Technologies and Crisis Instability

A key technology under active U.S. Air Force investigation aims to disaggregate the functions of key satellites onto multiple and overlapping small satellites. Such disaggregation would provide far more targets for an adversary to attack, assuming the disaggregated parts could communicate with one another and quickly switch off certain functions. If this wider distribution substantially increased the space architecture's resilience while maintaining sufficient combat effectiveness, it would mark a major step forward in promoting crisis stability in space, discouraging first-strike

attacks in space through the reduced vulnerability of satellite constellations. This option's success is hardly assured, though, and China and other adversaries would almost certainly pursue countermeasures.

More advanced ballistic missile defense (BMD) technologies have been and continue to be researched, with direct implications for space offense. Directed-energy weapons (DEW), probably ground-based, are one obvious example. If cost-effective and reliable DEW weapons could be developed, they would have important implications for ASAT capabilities: a much lower cost per shot compared with kinetic energy interceptors, a possible countermeasure to disaggregated satellite constellations, reduced space debris and collateral damage, and others. Ground-based DEW also could help to establish a more secure second-strike offensive space capability, given the difficulty of destroying such weapons in a country's homeland.

On the question of whether to reveal the existence of space weapons if they are developed, there is a clear tension between the respective benefits of opacity and transparency. As a rule, transparency is desirable in promoting a stable space environment. Yet risk aversion, which is generally stabilizing in a crisis, appears to be strengthened by uncertainty. A balance may be best: not enough transparency for an opponent to know it is weaker and thus has greater incentive to strike first in a crisis, but enough to concern the opponent about one's own capabilities.

Space Resilience

One way to reduce pre-emption incentives in a potential crisis is to reduce the effectiveness of an adversary first strike while establishing powerful countervailing capabilities in the other domains. An augmenting step is to ensure that one has a credible capability to retaliate against a first-striker's space assets after absorbing a first strike, assuming that an attacking power holds high-value space assets on which it depends.

A key dimension of both efforts is, if possible, to achieve substantial enduring resilience in one's space architecture, including ground C4ISR components as well as space assets. An enduring space resilience would largely blunt the effectiveness of an adversary's space offensive capabilities, greatly reducing space escalation incentives. If other major space powers also possessed space resilience, then the overall effectiveness and value of space offense would be greatly diminished, as any offense would likely fail to deliver the desired effects. Perfect resilience is not necessary, but the resilience should be sufficient to substantially increase the uncertainty of a successful space

attack, and thus likely magnifying risk aversion in an adversary. The disaggregation of space assets plays a major role in planning for space resilience. This growing emphasis on resilience also characterizes U.S. efforts in cyberspace. Achieving resilience through disaggregation may also involve "atmospheric satellites": high-endurance, in-theater unmanned aerial vehicles (UAVs) for ensuring connectivity and posing a major new challenge to an adversary's offense.

The potential effectiveness of space resilience measures ensures the development of countermeasures, and it is likely that the advantage of any given resilience approach will be more fleeting than final, barring unforeseen technological advances. The United States will likely be forced to confront Chinese resilience measures as well. While such a "resiliency competition" would have unclear effects on crisis stability, it undoubtedly would introduce more uncertainty into the calculations of space powers, potentially causing a mutual increase in stabilizing risk aversion tendencies.

International Options

In her chapter, Victoria Samson reviews several international and related options to strengthen crisis stability in space. She notes that the dual-use nature of space technology establishes user intent as a paramount concern, placing primary importance on transparency of intent and policies. International discussions can strengthen crisis stability through government-to-government relationships, establishing both emergency points of contact and a shared context for crisis decision-making. Voluntary norms of behavior and international treaties are each relevant approaches to encouraging transparent space activities, but the willingness of individual states to accept and abide by treaty mandates limits the latter option. Such international approaches to space stability are not mutually exclusive; they together demonstrate a strong commitment to ensuring that space remains usable over the long-term, and both can thus assist in the pursuit of national security and international stability goals. Any effort to signal good intent in a crisis would rely heavily on pre-existing relationships and on space behavior over preceding months or years. More can be done to reduce misunderstanding, such as expanding space and space security conversations to eventually involve all major space stakeholders, non-traditional partners, and emerging space actors.

Crisis/Conflict Signaling and Communication

In their chapter, Dennis Blair and Bruce MacDonald examine signaling and communication and their implications for crisis stability in space. They emphasize the importance of perceptions, which can cause the possibility for misunderstanding

and miscommunication between countries to rise in tandem with broader tensions. In peacetime, isolated space incidents are routine and rarely cause major problems, though they may result in heightened vigilance against possible repeated actions. In a crisis, both intelligence and military activities will intensify, and participants will examine each other's actions more guardedly with emphasis on divining intentions and possible signaling. Uncertainty over actions will run high in a crisis; actors may even be uncertain about the impact of their own actions. Dazzling an adversary's intelligence satellite with a laser may do more damage than expected, but the satellite's owner may well respond as though the instigator intended the full extent of the damage. The fog of war can easily creep into the vacuum of space.

Early moves into space conflict would likely be modest efforts to support military operations and signal the adversary. Space conflict appears unlikely to begin or remain purely in space; it would more likely evolve from earth- or cyber-based conflict. The challenge is to ensure that the message received is the same as the message signaled. Given the world's lack of experience in this new domain, there is a real danger that early signals will be misinterpreted, with serious implications for escalation. An ascending order of threatening space activities theoretically exists, though countries may rank such actions differently. In signaling, it is difficult to distinguish actions meant to communicate intent from those intended to degrade capability once true conflict is underway. Signaling an adversary in a crisis is fraught with potential danger, given the very high possibility of miscommunication. Chances for direct dialogue are rare in such circumstances, and even dialogue can suffer from misunderstanding. Pure military actions can convey implicit messages about intent and therefore have an important political dimension. Crisis diplomacy of whatever kind can generally benefit from previous peacetime dialogue among potential adversaries on space and space-cyber crises.

Conclusions

An inherent risk of strategic instability exists where relatively modest defense efforts create disproportionate danger to an adversary, as in space offense. In addition, a serious risk of crisis instability exists in space due to the potential payoff of "going first"—destroying an adversary's satellites before that adversary destroys one's own. Indeed, high strategic payoff from pre-emption virtually defines the term "crisis instability." While this report does not attempt to determine how a specific crisis would unfold, the potential for space instability appears high and likely to grow unless greater resilience can be built into space architectures.

Current space architectures offer strong incentives for space powers like China and the United States to avoid situations that may encourage an adversary to make a first major offensive strike in space. The disadvantages of attacking second rather than first appear to be substantial, placing a premium on striking first—and striking hard—in a crisis. Similar incentives exist in cyberspace.

The United States derives more military and economic benefit from space than China or any other country, though the margin of this benefit may decrease over time as China continues to strengthen its space capabilities. For as long as the United States derives more benefits from space than others, however, it has particularly large incentives to do all it can to maintain space stability and keep space free from offensive actions. An unstable space domain is and will likely remain contrary to U.S. security interests. This finding is reinforced by the reality that no country has significant experience in space conflict, and by the possibility that uncontrolled space escalation could endanger the military and economic advantages that space provides to the United States.

Uncertainty

At least five space uncertainty features will aggravate crisis stability:

- Rapid space/cyber technological change
- Unpredictable cross-domain interdependencies
- Major threat uncertainty
- Inexperience in space crisis management (the "sorcerer's apprentice" problem)
- Persistent uncertainty about attack effects

The United States and China are urged to prioritize avoidance of any unlimited strategic space and cyber conflict that would cripple the economies of both countries, a view voiced in numerous individual and group discussions. Even with no use of nuclear weapons, a major space attack would be amplified in impact by the nations' highly connected and interconnected economies, especially if the strike were coupled with comparably strategic cyber attacks. Despite this shared fear, the dynamics of a fluid and escalating crisis coupled with the unpredictable effects of such attacks could result in outcomes neither country would wish. In this dynamically unstable

crisis environment in space, combatant countries would likely share a significant level of space risk aversion that will have some deterrent effect against space escalation, precisely because the consequences of all-out space or space-cyber conflict would be so devastating. Such risk aversion is unlikely to be robust, however, and it could well fail without warning.

Resilience

Given the crucial contribution that space plays in U.S. conventional military power, and the PLA's apparent determination to develop a capability to diminish U.S. space assets should conflict break out, it is important for the United States to reduce incentives for an adversary to attack U.S. space assets in a crisis. The single most stabilizing step the United States can take in space is to develop and deploy a more enduringly resilient space architecture that can absorb a first strike and still deliver acceptable performance that provides U.S. forces and decision-makers with the information they need. A combination of highly disaggregated satellite architectures coupled with aeronautical and other backup systems appears to offer great promise.

A central question for the years to come will be the sustainability of any resilient space architecture that might emerge. Countries will have great incentive to overcome the space resilience of adversaries while maintaining their own. Space asset resilience is also important because it can reduce adversary incentives to initiate offense in space and escalate quickly. A non-resilient space architecture would offer major incentives to do just the opposite, as an adversary would benefit significantly from striking first and escalating ahead of any retaliation.

Achieving a resilient space architecture will not be a one-shot step but an ongoing struggle, as an adversary (or adversaries) will likely seek countermeasures to erode or subvert this resilience, given the crucial importance of space-enabled information services to U.S. military pre-eminence. In addition, the value of space architecture resilience means that the United States will likely be confronted over time with credible Chinese and other efforts to establish resilient space architectures of their own.

At least some level of offensive U.S. space capability is probably needed to maintain space crisis stability given the steps that China has already taken in this area, though with an important caveat. U.S. offensive space capability should not be so substantial that it triggers a major Chinese space offensive buildup, creating the kind of threat it wants to avoid. Obtaining an appropriate balance will be a delicate task that could be supported by mutual dialogue. Communication and dialogue with one's potential

space adversaries is essential, ideally in peacetime and certainly in a crisis. In a crisis, communication would be easier to conduct through pre-existing channels.

The United States and China should adopt a common goal to avoid strategic space and cyber conflict, which would devastate the economies of countries involved. In addition, the United States should exercise great caution in considering the first use of offensive space capabilities beyond minimal jamming. The country possesses military advantages in other domains, and the fact that it benefits more from space than other countries means it has more to lose in a potential space conflict.

While any use of nuclear weapons would pose a serious threat of escalation to full-scale nuclear war, any use of space or cyber offense would not in all cases pose a comparable escalation threat. That said, a series of reciprocal escalations could easily become unstable. No clear-cut escalation barrier exists in the space and cyber domains, and given the short-term tactical benefits of escalating ahead of an adversary, each additional escalation could create incentives for further escalation that an adversary would not always anticipate. Escalation in space, then, is likely a slippery slope with few off-ramps. Accordingly, great care must be exercised in considering escalation in space offense, with full recognition of the potential for unstable escalation.

Space Offense

Unless the United States can assure a robustly resilient space architecture capable of absorbing the strongest attack possible while still delivering acceptable performance to U.S. forces and decision-makers, the country will require some level of space offensive capability to deter adversary attacks in space. The United States could be forced in the absence of such a capability to respond to a bloodless adversary strike against U.S. space assets with a major casualty-producing attack, and few other early conflict actions go as far to invite further escalation.

From a strategic perspective, stability in space is likely tolerant of low-level offensive actions like jamming, highly intolerant of major strategic-level space offense, and highly uncertain in between. Uncertainty between the extremes depends on a space architecture's resilience: the less resilient the system, the more a lower-level space offense would threaten space stability.

Findings

Place Priority Emphasis on Developing a Resilient Space Architecture

Developing a more resilient space architecture and other backup approaches to securing U.S. assets in space and on the earth will pay major dividends in crisis stability, deterrence, effectiveness of U.S. military forces, and decision-making at senior leadership levels.

Develop Offensive Counter-Space Capabilities Consistent with U.S. National Space Policy for Primarily Deterrence Purposes

With a more resilient space architecture, the United States would benefit from having sufficient survivable offensive space capabilities. Such capabilities would prevent other space powers from believing they could achieve major "bloodless" military advantages while leaving a U.S. response choice of either major casualty-producing steps or cyber actions of less certain effectiveness. The U.S. objective would be to deter attacks on its space assets. An effective deterrent should be highly survivable and capable of negating adversary space satellite capabilities both reversibly and permanently. A strong diplomatic initiative to pursue a more stable space environment would complement the development of a survivable space deterrent.

Strengthen the Taboo on Attacking Nuclear Force-Supporting Infrastructure

Actions that indicate any interest in targeting the key space or cyber infrastructures that support any party's nuclear forces would be extremely destabilizing, suggesting—either accurately or inaccurately—that preparation for nuclear conflict is under consideration.

Encourage Greater U.S.-China Dialogue on Space

The single most important non-military option available in a crisis is to dialogue with the adversary country, and any crisis communication stands to substantially benefit from a precedent of prior discussions on related matters. Such exchanges allow participating parties to develop familiarity with each other and with the perspectives of adversaries.

Take Steps to Better Exploit Risk Aversion and Uncertainty to Maintain Space Stability

Risk aversion will play a growing role in space and cyber deterrence as the United States and China grow more economically dependent on space and cyberspace and become increasingly interdependent within the two realms. An effort to identify and encourage steps that increase risk-averse behaviors merits priority attention, as it would serve to encourage greater caution among adversaries.

Avoid Kinetic Offensive Counter-Space Capabilities

Any substantial use of kinetic energy ASAT weapons by either or both sides in a space conflict would produce vast amounts of space debris, wreaking tremendous and lasting damage on key orbits in space. Because such damage would have major economic and other consequences, this type of offense should be avoided if at all possible. The United States should seriously consider abjuring such weapons and initiating a public initiative urging China, and others, to do likewise, especially if we do not plan to use such weapons anyway.

Use More Extensive Crisis Gaming to Better Understand Space Crisis Dynamics

The U.S. Department of Defense should expand its space war-gaming exercises to include a full suite of space-oriented crisis games with the objective of gaining deeper insights into the behavior of the United States, China, allies, and others in a space crisis context, either apart from war games or as an important adjunct to them. Specific objectives could include the impact of different kinds of signaling in a crisis, the role of uncertainty, interaction between the space and cyber domains, and techniques to de-escalate in a crisis or in the early stages of actual conflict.

INTRODUCTION

The protection of national interests and maintenance of stability during crises is a longstanding issue among scholars and policymakers. While crisis stability in the land, sea, and air domains has been their traditional concern, the nuclear domain emerged as a focus seventy years ago and, more recently, the space and cyber domains have prompted growing interest. The military roles of space and cyber activities in the non-nuclear domains have grown substantially. Space plays an ever-increasing role as a "force multiplier" in providing and transmitting information, dramatically increasing the effectiveness of conventional weaponry and military decision-making. Accordingly, military space capabilities have drawn increased attention in many quarters, as have questions of stability and instability in space in a potential crisis. While both the United States and the Soviet Union had early ASAT systems,[1] the close relationship that their nuclear infrastructures had with satellites of military importance led to a de facto understanding that those satellites were off limits, at least in situations short of full-scale nuclear conflict. Their space assets, in other words, were protected by the threat of a nuclear response to any attack on so vital a component of their strategic architectures.

Probably no single event did more to thrust this issue into the public, and expert, consciousness as China's January 2007 ASAT test against an old Chinese weather satellite. The inherent threat of space conflict implied by the 2007 test had more direct impact than any other event on the minds of those concerned about national security, and it notably influenced the popular imagination. Yet space-based military threats have lurked for decades; since the mid-1980s, specialists have clearly recognized the trend toward greater military dependence upon satellites and space. In a remarkably prescient study, an important group of distinguished academics, former government leaders, and leaders-to-be[2] stated in early 1987 (based on their deliberations the year before) that:

> The long-term trend toward greater reliance on satellites by military units of all sorts appears to be irreversible. In consequence, ASAT deployments would create growing opportunities for crisis inflammation… Space-based

> portions of command systems would lose their immunity from non-nuclear attack. Under such circumstances, techniques for interfering with military space activities are likely to be employed in situations where that would not happen today [i.e., 1987]. *Space would therefore become a medium for exceptionally swift crisis propagation, and/or escalation* [emphasis added].[3]

It is possible today to repeat those far-sighted words with little change. The authors' recognition of the potential for "exceptionally swift crisis propagation, and/or escalation" has only grown more relevant, as space now plays a more important role in conventional conflict than ever before. Accordingly, the issue of space crisis stability requires national security specialists to better understand the strategic landscape and dynamics of space and how U.S. and allied interests can be preserved in this new and largely unfamiliar strategic domain.

Space stability, in its broadest sense, can be defined as a state in which space assets and their associated ground elements perform as intended on a day-to-day basis, and in which disincentives outweigh incentives for adversaries in a crisis to initiate offensive actions against space assets, or to escalate the scale of offensive actions if some level of offense is already under way. Such a condition is also characterized by a system's ability to absorb at least modest perturbations to the status quo without allowing their amplification over the course of a crisis or conflict.

Participating states may not identically perceive conditions in the space domain, and no state's perception may perfectly match with objective reality. This principle can manifest in many forms, some stabilizing and others destabilizing, which partly explains why "space situational awareness" is widely recognized as an important issue in the military space domain. It is conceivable, for instance, that one state may perceive a condition of stability in space where a less space-capable adversary would not. The more powerful state's escalation dominance would result in a "parochial stability" that offered no short-term incentive for escalation, but would prove unstable in the medium-to-long run if the weaker power sought to change the situation it found unacceptable.

In practical terms, the appeal of such parochial stability has much in common with the allure of a desert mirage, tempting thirsty travelers into the desert, and toward disaster. The very essential contribution of space as an economic and military force multiplier ensures that any major power, such as the United States or China, would be highly unlikely to allow a competitor to attain, much less sustain, such a dominant position. Either nation would expend any resources necessary to boost its own capabilities and counter the dominance of the other. Space dominance posed a less significant threat in an earlier era, when space was a far smaller factor in economic and national security planning, but those days are long gone. Until technology creates fundamental changes in the space domain, offense tends to have the advantage in space by its very nature. Because the technologies involved are becoming widespread, a monopoly on space power, or a position of serious space dominance, is neither credible nor sustainable.

The real challenge for the United States is how to achieve stability in space under current and likely future circumstances in ways that enhance U.S. and allied security interests while recognizing the legitimate security interests of other countries. The overall stability of space is and will remain a central component of crisis stability, unlike in previous decades, when the space domain was more secondary.

Overall stability, and crisis stability in particular, are highly desirable features for U.S. security interests in the space domain and generally also in cyberspace. As long as the United States continues to derive major economic and military benefit from what can be termed "space-enabled information services" (SEIS) and the larger information services of cyberspace, maintaining stability in space and cyberspace could allow the United States continued access to these benefits in times of crisis or conflict, when they would prove most valuable. Accordingly, strengthening our understanding of the dynamics of space deterrence and space stability in crisis situations is an essential national security task.

In a crisis, the decisions made by the United States and others on whether and how to use space control assets will play an important role in determining whether or how a crisis evolves and escalates. Understanding crisis stability in space, and to some extent in cyberspace, should accordingly be a high-priority national security objective, yet too little is known today about crisis behavior in either domain. There fortunately have been no notable space crises from which to extrapolate. While space war games offer insights, participants too often rush through the crisis phase of the game and into the conflict itself, which is usually of greater interest to the participants and even to the game controllers. The crisis period is often viewed in these games as a necessary but minor prelude to the main event, but this phase should be a key focus of attention. Understanding the dynamics of the space domain in a crisis is essential to understanding how to maintain stability in space and maximize the chances of a

successful outcome for U.S. interests while minimizing the chances of a potentially costly and lethal all-out space conflict, or even larger full-scale war.

This is not to downplay the importance of space war games, which can themselves offer important insights into the strategic landscape of space, but rather to emphasize that more, and perhaps separate, attention needs to be paid to the crisis phase. There is a rich vein of information to be mined from "crisis games," where the emphasis would be on understanding what behaviors, decisions, and actions prove to be escalatory or de-escalatory, whether or not the crisis leads to space conflict. But much more needs to be done, such as clarifying what features would lead to more informed, and informative, "crisis games" for space, in addition to war games.

Stability in space, especially during a crisis, assures continued U.S. access to the military and commercial information streams both generated in and transmitted through space, and it is thus an important contributor to U.S. national security interests. The 2010 U.S. National Space Policy states the challenge clearly and accurately:

The now-ubiquitous and interconnected nature of space capabilities and the world's growing dependence on them mean that irresponsible acts in space can have damaging consequences for all of us. [4]

Conflicts in space are likelier than geographically isolated conventional conflicts to have widespread collateral effects that reach across this increasingly interconnected world. It is incumbent on all who care about reducing U.S., allied, and world vulnerability to such irresponsible acts that we understand how such acts, and the unintended consequences of such acts, operate in the space domain. With this understanding, we can take steps to reduce this vulnerability, potentially averting a cycle of crisis escalation in which dire space actions would almost certainly prompt greater retaliatory actions (e.g., attacks on higher-value adversary satellites or casualty-producing strikes on ground facilities). The resulting stability would enable all nations to enjoy the substantial economic, military, and scientific benefits that modern space capabilities can provide.

BACKGROUND

Space has played an increasingly important role in U.S. security since the early Cold War. After initially gaining military significance for its role in ballistic missile trajectories, space assumed a new level of importance with the launch of military satellites that promised to provide crucial strategic intelligence on the nuclear forces of the Soviet Union. The Central Intelligence Agency's Corona program conducted surveillance of the Soviet Union, China, and other countries from 1959 to 1972, providing important classified imagery for multiple U.S. national security requirements. The military importance of space increased further with the development of satellites carrying other sensors and electronic listening devices, which it possible to gather new types of adversary information. The bulk of this new capability initially was directed at the strategic nuclear mission, not at conventional forces, but new capabilities became possible as space and other technologies rapidly improved. U.S. conventional weapons were already gaining capability through "smart" technology, and this accrual was accelerated by tactical intelligence from U.S. space assets. The United States displayed these new, robust capabilities to the world during the 1991 Gulf War, and over the last 15 years, in the Balkan states, Iraq, and Afghanistan.

Today, space plays a far broader economic and military role than during the Cold War. Still, the large and growing role that space plays as a foundational feature in U.S. conventional military capability, strategic nuclear posture, and the U.S. and world civilian economies remains largely under-appreciated among publics today. Space is an environment where satellite sensors collect key military and civilian data, and a medium through which military and civilian information is transmitted via satellites. With its GPS satellites and sophisticated intelligence collection systems, the United States is more dependent than ever before on SEIS. The vast and growing services of U.S. space assets provide allow diplomatic and military decision-making and weapons capabilities to be far more effective than in the past, resulting in vital advantages across the spectrum of potential conflict.

The United States and allied forces rely on satellite communications to carry out operations far from established terrestrial communication networks. Satellite communications enable long-haul intelligence, surveillance, and reconnaissance (ISR) data transmissions for systems such as UAVs; critical GPS information for joint forces; global/theater missile warning; timely weather information from satellites; and other services. Space greatly helps the United States to project power far from its territory, an important capability that its allies and friends rely upon and its potential adversaries must take into account. Without such capabilities, the United States would face far greater difficulty in functioning as a truly global power unmatched by any other country. China, Russia, and others have not overlooked the United States' space-enabled capabilities, and they appear to have reached certain security conclusions concerning U.S. dependence upon SEIS. U.S. space capabilities are critical enablers for joint forces, but they may become an American Achilles heel unless steps are taken to offset growing vulnerabilities in its space architecture. In 2007, then-commander of Air Force Space Command General C. Robert Kehler described the matter succinctly:

> The space capabilities we provide today are embedded in all of our combat operations. We cannot fight the way America fights without space capabilities. Space has become a contested environment, and we know that in any conflict our adversaries will try to deny us use of those space capabilities. [5]

It was likely inevitable that this vital component of U.S. military and economic security would in recent years draw the interest of potential adversaries looking for ways to pose a deterrence threat in peacetime and gain an asymmetrical advantage in conflict against the greater military strength of the United States and its allies. Much thought has been usefully devoted to how conflict in space might be conducted, with analysis and war games contributing to our understanding. To date, however, issues related to the nature of crisis stability in space—how countries might behave in space during a crisis, how such actions would be perceived and influence another country, the implications either for resolution of the crisis or aggravation of the crisis into space conflict, and how earth-bound dimensions of a crisis or conflict would influence crisis decisions in space—have received relatively little attention. The 2009 report of the Congressional Commission on the Strategic Posture of the United States noted the importance of these issues by urging the United States to "develop and pursue options for advancing U.S. interests in stability in outer space." [6] In addition, the 2010 statement of U.S. Space Policy "recognizes the need for stability in the space environment." [7] But still unclear are what factors contribute to space stability, how to achieve and maintain those conditions, and the primary threats to a stable space environment.

China, a rising international power with particular focus on the challenge of force-multiplying space capabilities, has greatly expanded its presence in space over the last twenty-five years. It is now a major space power, as seen by the fact that it leads every other country in total space spending except the United States, which still outspends China by almost a four-to-one margin ($40 billion to China's $11 billion annual outlay). [8] While such comparisons must recognize that a dollar may have greater purchasing power in China than in the United States, the difference in figures still suggests greater U.S. efforts. Though China is probably better known for civilian space achievements such as orbiting its own "taikonauts," it still puts great emphasis on the military dimensions of space power. Over the last ten to fifteen years in particular, China's military writings have shown a keen appreciation for the important role that space assets, and their supporting ground-based infrastructure, play in enhancing military capabilities. The country has further demonstrated this appreciation in its military acquisition programs and, most starkly, in its 2007 demonstration of an ASAT capability, when it shot down an old weather satellite using a ground-based interceptor. Meanwhile, Russia has shown a renewed interest in offensive space capabilities years after its first test of an ASAT capability, demonstrating through numerous recent statements an awareness of the key role that space plays in national security and its desire to assert itself on the global strategic stage. In addition, India has expressed serious interest in ASAT capabilities.

It is no wonder that China's PLA wants the capability to interrupt the rivers of information and services that U.S. space assets provide. This information has significantly increased the effectiveness of U.S. military decision-making, U.S. weapons, and especially U.S. war-fighters, creating vital advantages across the spectrum of potential conflict and major benefits to U.S. security interests. As a major and growing regional power, but not yet a global power like the United States, China has a strong interest in developing asymmetrical strategies that provide a capability to strike at U.S. military weak spots rather than strengths. The United States' critical dependence on its space assets is just such a vulnerability. The design of most U.S. space assets took place when space was a relative sanctuary and credible threats to these assets were minimal, an era now well in the past.

Though absolute U.S. advantages in space will increase over time, the margin of U.S. advantage seems likely to diminish as China, likely Russia, and possibly others increase

their space capabilities. In so doing, adversary military establishments will reap both the military advantages and vulnerabilities of greater space-enabled capabilities. It is possible for the United States never to become embroiled in a crisis with China, Russia, or another major space power in the coming century, and all sides should expend great effort toward this worthy goal. However, it would be risky to assume that such a crisis will never occur. A greater understanding of the space domain's landscape and dynamics of crisis stability and deterrence, and its interdependence with the cyber domain, will allow greater confidence in the management and decision-making of crises to come. The interactions and interdependencies between space and the other domains are vast and complicated, but at least some exploration of these interdependencies is essential to understanding crisis dynamics more generally in the twenty-first century.

Space is strongly linked with cyberspace in the respect that the military and economic benefits of space overwhelmingly derive from information that also moves through the cyber domain. (This integration affects information directly generated in space as well as data simply transmitted through space.) Space war games and studies have repeatedly demonstrated this space-cyber connection, making it important to also consider cyber dimensions of space behavior, especially in a crisis context. The task of understanding the dynamics of the space and cyber domains is greatly complicated by steady technological advances that, over time, are re-sculpting the strategic landscape of both domains. Technological change was and is an enduring feature of the strategic nuclear environment, but its pace is demonstrably faster in the space domain and, to an even greater extent, in the cyber domain. While a strict focus on crisis stability within the space domain may initially be useful for reasons of simplicity, it would be a serious mistake to stop there. Cross-domain interactions will be unavoidable, other than possibly in highly localized tactical situations.

Space assets, and the communications and cyber links that enable them to function, are the means by which essential national security information is either generated or transmitted. This information is the lifeblood of U.S. conventional military superiority and plays a key role in the U.S. strategic nuclear posture as well. As such, these space related assets would represent extraordinarily appealing targets to adversaries in any future conflict, and their relative vulnerability can provide dangerously attractive incentives for pre-emption in a crisis, potentially facilitating an escalation to war. Similar incentives exist in cyberspace as well.

It would be difficult for a potential U.S. adversary to directly challenge the military capabilities of the United States. If, however, an adversary were successful in defeating a key enabling component of U.S. military power, such as space assets, that adversary could seriously compromise U.S. military strength. Such an asymmetrical attack capability would clearly be of interest to U.S. adversaries, in much the same way that hostile Iraqi and Afghan forces have relied heavily on improvised explosive devices (IEDs) to attack U.S. forces at their weakest point, rather than challenge U.S. forces directly. As one space expert has put it, "were the United States to lose the advantages that its space assets provide, U.S. military forces would almost instantly be transformed from an information age military to an industrial age military." The attraction of offensive counter-space capabilities to China and Russia is clear and is reflected in their military writings.

Of course, space offense is not only of interest to potential U.S. adversaries. Reflecting in 2006 on the United States' major and growing economic and military dependence on space, the George W. Bush administration for the first time stated in U.S. space policy that U.S. space assets are "vital to our national interests." [9] This 2006 policy statement was accompanied by statements and rhetoric that indicated a strong interest in U.S. offensive space capabilities that seemed to emphasize war-fighting over deterrence as a strategic rationale. It is noteworthy that the 2010 Obama administration's version of U.S. space policy changed some of the Bush administration's rhetoric and placed more emphasis on deterrence; still, it notably retained the "vital national interests" language of 2006.

The United States generally is prepared to safeguard its "vital national interests" through extraordinary means, including the use of substantial or even overwhelming military force. This only underscores the prominent role that the space domain plays in the security posture of the United States. The United States has a clear interest in maintaining uninterrupted access to these capabilities, making clear the need for a benign and stable space environment coupled with redundant and backup capabilities to ensure U.S. interests in space. The Obama administration, following closely on previous space policy, identified the need for the United States to safeguard its space capabilities:

> The United States will employ a variety of measures to help assure the use of space for all responsible parties, and, consistent with the inherent right of self-defense, deter others from interference and attack, defend our space systems and contribute to the defense of allied space systems, and, if deterrence fails, defeat efforts to attack them. [10]

Prior to 2006, this "vital national interest" language had never been a feature of U.S. policy; its presence reflects the rapidly evolving strategic environment of the early twenty-first century. This changing environment presents a challenge for crisis stability in space and U.S. security interests. The United States' dependence on space diminishes the credibility of any U.S. threat to carry out an offensive space action against its near-peers in the domain, as such action would invite retaliation against its space "vital national interests." The United States, in short, has more to lose in space than its adversaries. Current U.S. space policy and strategy begins to address this potential vulnerability by embracing a space force doctrine of deterrence, asserting that the United States will have an offensive capability to deter attacks on its space and space-related ground assets. U.S. doctrine and strategy are unclear about when, how, and under what circumstances the United States might employ offensive space force. This language leaves plenty of room for the United States to develop and deploy space-oriented, though not necessarily space-based, weapons of its own, tacitly recognizing that space is also becoming a growing component of Chinese and possibly Russian military power. Notably, U.S. space policy states that any response to an attack against space systems may be asymmetrical in nature and not limited to the space domain itself, "but rather will occur at the time and place of our choosing."[11]

CHALLENGES IN THE EMERGING SPACE ENVIRONMENT

The Non-Military Space Security Challenge

It would be a mistake to focus strictly on military threats to space assets. In addition to the serious military challenges it faces in space, the United States must contend with non-military threats in space alongside all other space-faring nations. The subtlety of such threats does not diminish their importance, as the U.S. National Security Space Strategy of 2011 stresses:

> The current and future strategic environment is driven by three trends – space is becoming increasingly *congested*, *contested*, and *competitive*.[12]

One of the biggest non-military threats faced by all countries in space is the growth of orbiting debris. The growth of global space activity has increased congestion, especially in important orbital areas in space, and the proliferation of debris has shown no sign of stopping. NASA elaborated on the matter in a 2013 news release:

> There are more than 20,000 pieces of debris larger than a softball orbiting the Earth. They travel at speeds up to 17,500 mph, fast enough for a relatively small piece of orbital debris to damage a satellite or a spacecraft. There are 500,000 pieces of debris the size of a marble or larger. There are many millions of pieces of debris that are so small they can't be tracked. Even tiny paint flecks can damage a spacecraft when traveling at these velocities. In fact a number of space shuttle windows have been replaced because of damage caused by material that was analyzed and shown to be paint flecks.
>
> "The greatest risk to space missions comes from non-trackable debris," according to Nicholas Johnson, NASA's chief scientist for orbital debris.[13]

There are an estimated five hundred thousand objects between one and ten centimeters in diameter, a size that can damage or destroy satellites. The particles smaller

than one centimeter exceed one hundred million in number, and they are still capable of inflicting serious damage on orbiting satellites. [14]

Today's space environment contrasts with earlier days of the Space Age in which only a handful of nations needed to be concerned with congestion. Now there are approximately 60 nations and government consortia that own and operate satellites, in addition to numerous commercial and academic satellite operators. This congestion—along with the effects of operational use, structural failures, accidents involving space systems, and irresponsible testing or employment of debris-producing destructive ASATs—is complicating space operations for all those that seek to benefit from space.

Increased congestion was highlighted by the 2009 collision between a Russian government Cosmos satellite and a U.S. commercial Iridium satellite. The collision created approximately two thousand new pieces of trackable space debris, [15] adding to the more than three thousand pieces of debris created by the 2007 Chinese ASAT test. These two events alone greatly increased the cataloged population of orbital debris.

The radio frequency spectrum is another area of increasing congestion. Demand for radio frequency spectrum to support worldwide satellite services is expected to grow commensurate with the rapid expansion of satellite services and applications. As many as nine thousand satellite communications transponders are expected to be in orbit by 2015. As the demand for bandwidth increases and more transponders are placed in service, there will be greater probability of radio frequency interference and more strain on international processes to minimize that interference. [16]

It is important to note that radio frequency interference is a problem just within U.S. space operations because of increasing satellite congestion. The head of Air Force Space Command, General John Hyten, has stated that through most of 2015, there were 261 cases where we have inadvertently jammed our own satellite links to ground stations. [17]

An unclassified summary of the 2011 U.S. National Security Space Strategy describes a related challenge:

> Space is increasingly competitive. Although the United States still maintains an overall edge in space capabilities, the U.S. competitive advantage has decreased as market-entry barriers have lowered… The U.S. technological lead is eroding in several areas as expertise among other nations increases. International advances in space technology and the associated increase in foreign availability of components have put increased importance on the U.S. export control review process to ensure the competitiveness of the U.S. space industrial base while also addressing national security needs.
>
> U.S. suppliers, especially those in the second and third tiers, are at risk due to inconsistent acquisition and production rates, long development cycles, consolidation of suppliers under first-tier prime contractors, and a more competitive foreign market. A decrease in specialized suppliers further challenges U.S. abilities to maintain assured access to critical technologies, avoid critical dependencies, inspire innovation, and maintain leadership advantages. All of these issues are compounded by challenges in recruiting, developing, and retaining a technical workforce. [18]

Military Space Security Challenges and Threats

The growing importance of space to military and economic security means that space has emerged as a key domain where national interests may collide under certain circumstances, with conflict a looming possibility. The 2011 U.S. National Security Space Strategy explains:

> Space is increasingly contested in all orbits. Today space systems and their supporting infrastructure face a range of man-made threats that may deny, degrade, deceive, disrupt, or destroy assets. Potential adversaries are seeking to exploit perceived space vulnerabilities. As more nations and non-state actors develop counter-space capabilities over the next decade, threats to U.S. space systems and challenges to the stability and security of the space environment will increase. Irresponsible acts against space systems could have implications beyond the space domain, disrupting worldwide services upon which the civil and commercial sectors depend. [19]

James Clapper, the U.S. Director of National Intelligence, elaborated in a 2015 prepared statement to the Senate Armed Services Committee:

> Threats to US space systems and services will increase during 2015 and beyond as potential adversaries pursue disruptive and destructive counter-space capabilities. Chinese and Russian military leaders understand the unique information advantages afforded by space systems and services and

> are developing capabilities to deny access in a conflict… China has satellite jamming capabilities and is pursuing anti-satellite system… Russian leaders openly assert that the Russian armed forces have anti-satellite weapons and conduct anti-satellite research. [20]

China presents the most prominent military space challenge to the United States. According to the U.S. Department of Defense, "China is developing a multi-dimensional program to improve its capabilities to limit or prevent the use of space-based assets by adversaries during times of crisis or conflict." [21] These capabilities include direct-ascent kinetic kill, directed-energy weapons, and satellite jammers. [22] Under Secretary of Defense Frank Kendall assessed in 2015 that the threat to the United States in space is, in his words, "particularly bad" due especially to Chinese and Russian advances in space offense capabilities. [23] His sobering assessment: By 2025, the U.S. posture in space would be its most seriously threatened position in any military domain. [24]

With conventional U.S. military power so dependent upon SEIS, China possesses substantial incentives, absent other considerations, to seek an ability to attack U.S. military space infrastructure. Its anticipated interest increases the military and economic roles of "near space," a region this report will define as the volume surrounding the earth from an altitude of sixty-two miles [25] out to geosynchronous orbit (22,200 miles). While many think of space as the "final frontier," for all intents and purposes, rapid growth in economic, military, and scientific activity has transformed this "near space" into a bustling region of civilization, its early frontier days increasingly a fading memory.

The United States likewise would have certain incentives—as well as strong disincentives—to execute a space first strike in a crisis. A more vulnerable U.S. space architecture could create greater incentives for the United States to strike while it still can function, disabling and/or destroying adversary offensive space capability. While resisting this temptation to attack may be regarded as morally virtuous, it could be strategically unwise for any space power. Attacking first in a space conflict appears to offer many advantages over responding to a space first strike; the latter option would necessitate the use of degraded forces against an opponent fully expecting such a response, and therefore is likely to be militarily and strategically undesirable.

Given that the PLA's military writings suggest it is well aware of this principle, as discussed below, a developing crisis would include substantial incentives for escalation. One potential mitigating factor remains a major unknown: the survivability of a country's offensive space capabilities after absorbing the full force of an adversary

first strike. If offensive space capabilities could be devised that did not themselves depend upon SEIS, the development of such capabilities may reduce the incentives to conduct a space first strike in a crisis. However, it does not appear likely that a major attack or retaliatory strike could be executed without such SEIS resources. A key consideration is the extent to which SEIS assets could incorporate resilience and "graceful" degradation—that is, degradation that is gradual and not inflicted over a short period of time. Strikes by non-near-peer adversaries that have few or no space assets could be addressed in traditional ways, though because the United States is unlikely to suffer direct casualties from a space attack, U.S. policymakers should probably give preference to retaliatory options that produce as few casualties as possible for an adversary like this.

As technology advances, the options for interfering with, disrupting, or destroying information streams in space or supporting space systems will likely increase, as will dependence upon such systems by the United States and others. While the United States should respond to such threats by pursuing defensive options for its space assets where appropriate, most observers believe that an offensive deterrent capability has a decided advantage in space over direct defenses, barring a defensive technology breakthrough or the development of very highly resilient, highly decentralized space systems that can absorb an all-out strike and still deliver SEIS capabilities. Precisely what such systems would look like is unclear, though they could involve a large constellation of disaggregated and fully interactive satellites in place of one or a few complex satellites. To remain resilient, such an architecture would likely change over time in response to adversary countermeasures.

During the Cold War, the inability of defenses to credibly blunt offensive nuclear threats was generally seen as stabilizing. Though distasteful, mutual nuclear deterrence resulted less from a strategic decision than from a recognition that any defense against nuclear attack could be easily overwhelmed, leading to a nuclear war that would kill millions on both sides. No comparable assured second-strike capability exists for the space domain at present, and space deterrence therefore is more likely than nuclear deterrence to fail during a crisis. To prevent the potential decisive advantages offered by a first strike from creating the conditions for serious instability, offensive counter-space capabilities (OCS) must somehow be kept limited in their use and survivable. In certain respects, offensive capabilities in the contemporary space domain closely resemble nuclear assets in the early days of the nuclear era, when all weapons were themselves vulnerable to a surprise first strike.

Offensive nuclear capabilities only became a stabilizing force after assured second strike capabilities emerged in the 1960s through the development of early-warning systems and sea-based nuclear missiles. The largely bomber-based U.S. nuclear deterrent of the late-1940s and most of the 1950s was always more vulnerable to surprise attack than silo- or sea-based ballistic missiles, and a greater incentive to conduct a nuclear first strike existed then as a result.

While the United States generally has led the way in utilizing space to enhance its military capabilities, other countries, especially China and Russia, have taken note of the military and other benefits that space provides and have developed important capabilities of their own, as noted earlier. They show no signs of slowing their efforts, which are largely directed toward the United States as their major perceived potential adversary. China has presented the chief challenge for the United States over the last twenty years, though Russia, drawing on its Cold War space legacy, should not be overlooked. Russia has also stepped up its interest in offensive space capability, recognizing, as has China, that space potentially offers an asymmetric means to weaken U.S. military capabilities in a conflict. India, Canada, and European Union countries are also worthy of note, though as U.S. allies and friends rather than as potential adversaries.

China sees space and cyber capabilities as highly important in meeting its need to potentially deter and, should deterrence fail, defeat the United States through attacks on points of military vulnerability. Because China perceives U.S. space and cyber assets to be vulnerable, it is no surprise that the PLA has developed capabilities in this direction and will likely continue to do so, despite rhetoric to the contrary. Probably of greatest interest to China is a capability to deter or defeat a U.S. attack growing out of a Taiwan Strait crisis, though other goals are possible.

China publicly states it has no interest in acquiring offensive space capabilities, yet its actions belie its public statements. As noted earlier, it successfully tested an ASAT weapon against a defunct Chinese weather satellite in 2007, and it has since conducted ostensible BMD and other tests that some analysts and officials have considered a cover for ASAT testing. Both ASAT and strategic BMD rely on hit-to-kill and related technologies to function. The technologies behind both are similar, as the United States demonstrated in 2008 when it used a Standard Missile 3 (SM-3) interceptor to shoot down an errant U.S. satellite in an operation codenamed Burnt Frost. On July 23, 2014, China tested a missile in what the United States believed to be an additional ASAT test. "Despite China's claims that this was not an ASAT test; let me assure you the U.S. has high confidence that the event was indeed an ASAT test," according to Deputy Assistant Secretary of State Frank Rose. Rose went on to note that Russia was also developing such capabilities.[26] In this context, it is noteworthy that, on the sixtieth anniversary of China's air force in 2009, its commander, Xu Qiliang, stated that military operations in space are a "historical inevitability and a development that cannot be turned back… only power can protect peace."[27] It appears that the PLA views space as a potential battlefield domain like any other, though this does not mean that China's political leaders take a less nuanced view of the space domain than their U.S. counterparts.

In understanding the Chinese challenge to U.S. security interests in space, it is important to remember that China believes it faces a particular challenge from the United States in the space realm. A 2015 Rand Corporation study describes China's perspective:

> Many Chinese analysts believe that China's space systems face a variety of potential threats. Some Chinese strategists appear to believe that other countries are actively developing counter-space capabilities that could threaten Chinese satellites, given what they characterize as a long history of anti-satellite weapon research, development, and testing in the United States and Russia dating back to the Cold War.[28]

China has great respect for U.S. military and civilian space abilities and accomplishments, and it is uneasy about U.S. military space capabilities going forward. As noted earlier, the United States spends about four times as much on space as China, and the United States has substantially more experience in space operations. China likely does not seek conflict with the United States, in space or in any other domain, but it wants to be prepared in case conflict someday appears inevitable.

From a Chinese perspective, the United States likely appears to possess an offensive space capability that extends far beyond mere satellite jamming, whether or not this is in fact true. China is highly suspicious of the U.S. Air Force X-37B, an unmanned maneuverable space vehicle that remains in orbit for twelve months or more at a time, and which to China seems to have an inherent offensive capability. Chinese suspicions have likely been heightened by the fact that the Air Force has released no information about the X-37B. In addition, the Air Force's recently-deployed Geosynchronous Space Situational Awareness Program (GSSAP) is able to examine orbiting assets and could appear to have offensive potential. Further, any suspicion of GSSAP may extend to U.S. commercial programs for on-orbit servicing of satellites, a growing business that springs from understandable commercial motives to extend the lifetimes

of costly satellites. GSSAP envisions rendezvous capabilities to get the best images of potential adversary satellites, [29] and on-orbit servicing by definition would involve GSSAP making close contact with a satellite to accomplish the servicing mission. According to NASA, "Robotic servicing in GEO [geosynchronous] orbit is inevitable… NASA will make its future large space observatories robot-serviceable." [30] More than two hundred communications satellites scheduled to exhaust their on-board fuel by 2022 could become candidates for life extension through on-orbit servicing, hence the business interest. [31] From a worst-case Chinese perspective, both of these sensible applications for GSSAP and on-orbit servicing may appear to be just a short step away from a possible offensive use, even if none is intended. Such capabilities provide important deterrence benefits even if they remain entirely peaceful, but they undoubtedly also add motivation for Chinese development of offensive counter-space capabilities.

While China may see itself as inferior to the United States in certain respects, it recognizes the value of the potential offensive space capabilities that the United States is now expanding. China, for this reason, can be expected to continue its own counter-space capability development. Chinese analysts view counter-space capabilities as useful not only for disrupting an adversary's military operations by exploiting potential vulnerabilities in its space systems, but also as an important contribution to strategic deterrence, according to the authoritative Science of Military Strategy, the hallmark publication of the PLA Academy of Military Sciences. [32] Little doubt exists that deterrence is part of the motivation behind China's development of offensive space capabilities. "Under the conditions of American strategic dominance in space, reliable deterrence in space will decrease the possibility of the United States attacking Chinese space assets," according to one Chinese analyst. [33] U.S. thought on potential conflict with China is weighed upon heavily by the threat of losing the vulnerable, costly, and difficult-to-replace national security satellite constellations that are key to U.S. military power. The United States must successfully resolve this challenge through both military and diplomatic means.

In short, the United States and China are both moving into a space arms competition that neither may want but neither appear to know how to avoid, given the role of space assets in providing or delivering tactical and strategic information that is of central, crucial importance to twenty-first century military success. For a comparable reason, military activities in cyberspace appear to be set on a similarly competitive trajectory. Neither China nor the United States may want to fall into this "competition trap," but neither power believes it can afford not to participate.

China appears to recognize the United States' overall space superiority, and its current great strides to narrow this gap are made easier in a critical respect: because China has yet to gain the global power status of the United States, it can limit its competitive focus to issues that concern its immediate surroundings. Conversations with specialists in both China and the United States make clear that China's prime focus is on regional influence and power projection, as it has seen little need to date for major force projection capabilities outside of Asia. Thus, China can focus its security space efforts on East and South Asia while the United States must maintain global reach, to some degree reducing the impact of U.S. space superiority. In any potential conflict with the United States, China presumably would prefer to avoid giving the United States time to marshal its forces and transport them to East Asia. Accordingly, if China perceived an ambiguous, subjectively defined threshold to have been crossed during a crisis, the delay to any reinforced U.S. military presence would give Beijing one more incentive to escalate in space (and in cyberspace as well) and to strike relatively quickly. After perceiving escalation as unavoidable early in this process, China would likely want to hamper U.S. force deployments and diminish the effectiveness of U.S. forces already in the region through strikes against U.S. Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) capabilities. To delay such strikes would only allow the United States to increase its own striking power against China. Important disincentives for escalation certainly would also be present, but the military advantages of space escalation could prove irresistible in a crisis or early conflict.

Yet China probably would prefer to avoid such action if it could resolve the crisis in a manner it found at least modestly acceptable. In the absence of highly compelling reasons for conflict, China would not place its economic wealth and strength at serious risk by opting into a major combat engagement not only with the United States, but probably also some or most of its allies. If China took this route, however, it likely would strike U.S. space and cyber assets early and hard in an attempt to disrupt and paralyze as much of the U.S. C4ISR network as quickly as possible. These are the systems that at early stages enable and reinforce U.S. regional superiority. The goal of the PLA, as a private U.S. research firm noted in 2009, would be to fight "quick wars with quick resolutions" if at all possible. [34] Any delay, in the PLA's view, would allow "a more strongly armed opponent such as the United States to eventually bring the full might of its military to bear." [35] Indeed, some in China believe that a conflict across multiple domains might begin in space, given its essential role as a military "center of gravity."

Chinese military writings emphasize the advantage of executing a first strike in a deteriorating crisis. "Adhering to striking after the enemy has struck… will make it difficult to realize the goal of preserving counterstrike forces. This is especially true when the technology levels of the two sides are greatly disparate. If a side does not seize the initiative before a war starts, once the war erupts, then it will be even more passive." [36] China appears to still adhere to a policy of active defense, described by Chairman Mao Zedong as "offensive defense or defense through decisive engagements." [37] There is little operational difference between an offensive strategy and China's active defense strategy, but the latter approach has the important distinction of initiating offense only in response to perceived preparations by an adversary to strike. If China determined that an adversary attack may be imminent, the country would likely strike first to reap the associated advantages. "Based upon this, active defense is best thought of as a politically defensive but operationally offensive strategy in which China will rhetorically maintain a defensive posture up until the time that war appears imminent… Central to the need to conduct offensive operations at the beginning of a campaign is the requirement to seize the initiative." [38]

China, like the United States, is growing more dependent on space assets with each passing year, as its overall military capabilities and ambitions continue to increase. Chinese leaders will likely use electro-optical satellites to monitor U.S. naval force deployments and movements, particularly those of carrier battle groups, long before they move close to China or Taiwan. A reliance on satellite reconnaissance would encourage China to refrain from attacking too early in a crisis, as any retaliation against Chinese satellites could eliminate access to information on battle group formations outside the range of its land-based aircraft. These satellites, and their associated support facilities, will represent an important and growing vulnerability that China will need to address.

While Chinese military writings provide important perspective on PLA thinking about the roles of space and space offense in a potential crisis or combat scenario, it is essential to note the crucial gap dividing these analyses by mid-level military officers from the high-level decisions ultimately reached by political authorities. Short of the direst circumstances, Chinese political leaders appear highly unlikely to risk China's economic gains of the last forty years to initiate war against the combined might of NATO, Japan, and other advanced nations. The Politburo Standing Committee of the Chinese Communist Party and the Chinese Central Military Commission would play exceptionally important decision-making roles in a crisis, while the PLA would

carry out decisions by these bodies. The PLA's role in a crisis would not be to act independently, though deviation from orders would be possible at lower levels.

Like their mid-level U.S. counterparts, Chinese military officers can advocate positions that do not necessarily reflect PLA thinking, much less official Chinese thinking. Some foreign observers believe that because PLA officers cannot distinguish themselves in combat—China has very limited actual military combat experience—ambitious officers attract notice to themselves through the ideas they express in writing. Whether such ideas reflect broader institutional thinking is difficult to determine. Chinese political leaders are likely well aware that their country possesses little recent combat experience; it last fought in the 1979 Sino-Vietnamese War, which was only a brief border war that lasted less than a month. In contrast, the United States has had substantial experience participating in modest- and large-scale combat activities over the last 50 years, giving it an intangible but significant advantage that Chinese leaders would be unlikely to ignore when considering engaging in conflict with the United States.

Chinese space security specialists are keenly aware of U.S. military space capabilities and privately acknowledge U.S. superiority in space. They claim that, as in the nuclear domain, China would tolerate a certain level of U.S. space superiority that did not threaten to develop into space dominance. While China likely does accept some degree of U.S. nuclear superiority, it is less clear whether this stance accurately reflects senior-level Chinese thinking about space. A superior nuclear force offers, at best, only modest benefits beyond the level of capability that guarantees an overwhelming physical effect on an adversary. Meanwhile, the possible large number of space targets and countermeasures may well offer more significant technical advantages to possessing superior capabilities and numbers of assets for offense in the space domain, though this correlation is not fully confirmed. Furthermore, while nuclear weapons serve mostly as a deterrent force and are not widely seen as war-fighting weapons, the potential role of offensive space capabilities is not limited to deterrence. Deterrence is more likely to fail in the space domain than in the nuclear domain, given the more "granulated" nature of potential space attacks and the ability of a modest space offense to inflict less direct devastation.

The discussion of military threats to space or ground space assets generally focuses on kinetic or laser attacks, but the cyber domain presents another important and growing challenge to U.S. and other space capabilities. Cyberspace contains direct and indirect avenues to disrupt satellite ground stations and their supporting infrastructure.

Satellite terminals for commercial communications are also quite vulnerable, as a 2014 technical white paper on satellite communications (SATCOM) security pointed out: "malicious actors could abuse all of the [SATCOM terminal] devices within the scope of this study. The vulnerabilities included what would appear to be back-doors, hard-coded credentials, undocumented and/or insecure protocols, and weak encryption algorithms. In addition to design flaws, [the authors] also uncovered a number of features in the devices that clearly pose security risks."[39] While these findings apply only to certain commercial SATCOMs, comparable threats are likely relevant to other components of military and civilian space architectures.

In remarks delivered in early 2016 to the Senate Armed Services Committee, the Director of National Intelligence, James Clapper, gave a succinct assessment of the challenges to U.S. space interests:

> Threats to our use of military, civil, and commercial space systems will increase in the next few years as Russia and China progress in developing counter-space weapon systems to deny, degrade, or disrupt US space systems. Foreign military leaders understand the unique advantages that space-based systems provide to the United States. Russia senior leadership probably views countering the US space advantage as a critical component of war-fighting. Its 2014 Military Doctrine highlights at least three space-enabled capabilities—"global strike," the "intention to station weapons in space," and "strategic non-nuclear precision weapons"—as main external military threats to the Russian Federation. Russia and China are also employing more sophisticated satellite operations and are probably testing dual-use technologies in space that could be applied to counter-space missions. We already face a global threat from electronic warfare systems capable of jamming satellite communications systems and global navigation space systems. We assess that this technology will continue to proliferate to new actors and that our more advanced adversaries will continue to develop more sophisticated systems in the next few years. Russian defense officials acknowledge that they have deployed radar-imagery jammers and are developing laser weapons designed to blind US intelligence and ballistic missile defense satellites…
>
> Russia and China continue to pursue weapons systems capable of destroying satellites on orbit, placing US satellites at greater risk in the next few years. China has probably made progress on the anti-satellite missile system that it tested in July 2014. The Russian Duma officially recommended in 2013 that Russia resume research and development of an airborne anti-satellite missile to "be able to intercept absolutely everything that flies from space."[40]

In the following section, Dean Cheng describes how China's military leadership appears to view the role of space in coming years, and he places those perspectives in a larger political-military context.

Space and the Evolving Chinese Military

Dean Cheng

Introduction

The conclusion of the third plenum of the 18th Chinese Communist Party (CCP) Congress in late 2013 marked thirty-five years since the CCP had first begun to pursue the policies of "Reform and Opening." In the intervening time, China had evolved from an autarkic state whose military could barely reach beyond its immediate borders to a global trading power, the second largest economy in the world, and a military increasingly capable of operating not only throughout Asia but globally.

The PLA's steady modernization, made possible through nearly two decades of annual double-digit increases in its announced defense budget, has been partly intended to meet China's expanding obligations and address what the country perceived as a global military transformation. The emphasis on space capabilities has been particularly notable. Foreign wars of the past two decades have convinced the PLA that the ability to exploit information will be decisive in future conflict, and China must therefore be able to fight and win "local wars under informationized conditions." This capability requires the ability to gain information dominance (*zhi xinxi quan*), which in turn demands establishing space dominance (*zhi tianquan*).

Evolving PLA Responsibilities

Because the PLA is the armed wing of the CCP rather than a national military, its foremost task is to preserve the party's control while its secondary duty is to protect the national interests of the People's Republic of China (PRC). Hu Jintao underscored this dual role in 2004, two years after he became China's president and CCP general secretary. In that year, he assumed the chairmanship of the Central Military Commission (CMC), the highest body of the PLA and a counterpart to both the U.S. Department of Defense and the Joint Chiefs of Staff. As CMC chairman, Hu Jintao would be aware of the PLA's major programs and tasks.

In December 2004, Hu gave a speech where he outlined the "historic missions of our military [the PLA] in the new phase of the new century (*xinshiji xinjieduan wojun lishi shiming*)." In issuing these "new historic missions," Hu essentially provided the PLA with the highest-level description of its ultimate responsibilities:

- Guarantee the CCP's continued rule. As a party army, the first and foremost role of the PLA is to ensure the security of the CCP's rule against any foreign or domestic challenge.

- Safeguard national economic development through defense of sovereignty, territorial integrity, and domestic security. National economic development will remain China's priority for the foreseeable future, but without a strong foundation of security, such efforts will always be potentially vulnerable. Therefore, the PLA must provide for China's national security, even as resource allocations remain focused on national economic development. Particular focuses of this role are to prevent any attempt at secession or separatism by entities such as Taiwan, and to defeat any external attempt to aid and abet such efforts.

- Safeguard China's expanding national interests by providing strategic support. Developments in high technology mean that the PLA must expand its focus beyond traditional land frontiers. This task specifically includes preserving Chinese access to space (taikong) and the electromagnetic sphere, as well as ensuring China's ability to preserve its interests in the maritime domain.

- Help to ensure world peace. World peace and common development are prerequisites for China's continued national development, and therefore they must be maintained. For the PLA, this means greater engagement in activities such as United Nations (UN) peacekeeping operations (which also aids in the development of out-of-area operational experience).[41]

The importance of these "new historic missions" is reflected in their incorporation into the Chinese constitution in 2007.[42] Even more telling, they were part of an extensive education program administered to the entire PLA, ensuring that their importance was clear to the rank and file of the entire armed forces.

Within this context, explicit calls by Chinese military leaders, including strategists and doctrinal developers, for the establishment of "space dominance" reflect the importance of space for Chinese national security. Space-based systems are becoming

increasingly central to the rapid collection, accumulation, and transmission of information that is integral to various aspects of power, such as economic development, social stability, and military operations. Consequently, space is seen as the "high ground" for the pursuit of national interests, requiring the development of a strong "strategic space power (*kongjian zhanlue nengli*)" and the ability to establish space dominance.[43]

China sees a fierce, long-running competition for control of space dating back to the very beginning of the Space Age. In the Chinese view, the United States and Soviet Union both pursued military ends with their space programs from the outset, making space part of their Cold War confrontations. Their space conflict was largely indirect in the sense that it focused on the deployment of various types of satellites, but even then, both sides were conducting research into anti-satellite capabilities.[44]

The end of the Cold War did not lessen the importance of space dominance in China's view; instead, the "local wars" fought since 1991 have only underscored the domain's growing role. In the 1991 Gulf War, the United States and its partners brought some seventy satellites to bear against Iraq. These, according to PLA estimates, provided the United States with 90% of its strategic intelligence and carried 70% of all transmitted data for coalition forces.[45] In the Balkan conflict of the 1990s, NATO forces are assessed to have employed some eighty-six satellites, which provided a dense, continuous flow of real-time data, allowing the NATO forces to precisely target Serbia's main military assets for sustained, coordinated strikes.[46]

Since then, space has assumed even greater importance. Consequently, as one recent Chinese analysis concluded, the superior military space power will enjoy decisive benefits. As the new high ground of international strategic competition, space may change the basic context of international military conflict. This possibility poses a serious challenge to Chinese security.[47]

Evolving PLA Doctrine: Rise of Jointness

Securing space dominance is not only a strategic-level task for the PLA, but it is also an essential operational-level objective reflected in Chinese military doctrine. In 1999, the PLA thoroughly revised its operational guidance with a new series of manuals and regulations that constituted the "New Generation Operations Regulations." This wholesale revision of operational doctrine affected every aspect of the PLA, from its conception of future wars to its training and organization.

The issuance of these new regulations occurred during what the PLA perceived as a global military transformation (junshi biange) of the character of modern wars, from "local war under modern conditions" (i.e., industrial-era warfare) to "local war under modern, high-technology conditions," and subsequently to "local wars under informationized conditions." Local wars under modern, high-technology conditions exhibit several key characteristics.

- The quality as well as the quantity of weapons matters. The side with more technologically sophisticated weapons will be able to determine the parameters of the conflict and effectively control its scale and extent.

- The battlefields associated with such conflicts are three-dimensional, and they extend farther and deeper into the strategic rear areas of the conflicting sides. Consequently, military operations will occur over an ever-broader physical space (including outer space), with fewer and fewer areas out of an opponent's potential reach.

- The conflict is typically marked by high operational tempos conducted around the clock, under all-weather conditions.

- The fundamental approach to warfare is more complex. Local wars under modern, high-tech conditions not only incorporate operations typical of local wars under modern conditions, but also place much greater emphasis on joint operations, while also incorporating more aerial combat, long-distance strike, and mobile operations.

- Finally, the role of command, control, communications, and intelligence (C3I) is paramount. C3I functions are essential to successful implementation of such wars; consequently, the ability to interfere with an opponent's C3I functions also is much more important.[48]

In order to successfully engage in local wars under modern, high-tech conditions, the PLA promulgated the "campaign basic guiding concept" of "integrated operations, key point strikes." This idea provides the fundamental theoretical basis for planning and organizing military campaigns, directing campaign training, planning weapon system and equipment research and production, and enunciating modern campaign practices.[49]

"Integrated operations" refers to the idea of integrating forces, domains, and activities. Ideally, the planning and conduct of campaigns should be undertaken as a holistic, integrated effort, with the participating forces, areas of operation, and types of activities all contributing towards a common objective, leading to victory. "Key point strikes" emphasizes the importance of concentrating best available forces for attacks against the adversary's greatest vulnerabilities at central moments in the campaign—especially at the outset, because recent wars often have ended after only one campaign.

"Key point strikes" usually would target those parts of the enemy's forces and infrastructure that bind together the "system of systems" that comprise modern militaries, effectively preventing them from effective inter-operation. Typical "key points" include an opponent's C3I infrastructure, including reconnaissance and surveillance systems.

Given the types of wars the PLA may likely wage, the campaign basic guiding concept, with its emphasis on "key point strikes," was moving space to a more central role in PLA doctrine by the end of the twentieth century.

The ability to implement "integrated operations, key point strikes" relies on joint operations. Indeed, regulations governing joint operations were apparently the capstone of the New Generation Combat Regulations, taking precedence over campaigns of individual services.

For the PLA, "joint campaigns" are defined by four criteria:

- The campaign involves two or more services

- Each service contributes a juntuan-level of force (i.e., a group army, a military region air force, a fleet, or a Second Artillery base)

- The campaign has a single, unified command structure

- The command structure develops a single, unified campaign plan, which all the participating forces will follow[50]

The unified command structure is of special importance to the conduct of joint campaigns. It not only plans and implements the campaign plan, but it also helps to coordinate information drawn from sensors, weapons, and other platforms, ensuring

that there is a common situational picture. Space systems are essential in acquiring and transmitting this information.

Evolving PLA Doctrine: Rise of Informationization

Even as the PLA promulgated its new regulations, it recognized that warfare continued to evolve. PLA analysts spent significant time examining NATO operations in the Balkans, the U.S. war in Afghanistan, and the coalition war against Iraq in 2003. It is not clear whether these analyses have led to changes in the New Generation Combat Regulations, but they appear to have affected other aspects of PLA thinking about future conflicts.

In PLA analyses, the two decades after the first Gulf War were best characterized by a growth of information and associated technologies. The current Information Age, in contrast with the Industrial Age of the twentieth century, has not only seen the reorganization of industrial and social institutions to accommodate the growing importance of information, but has also affected the conduct of warfare. Just as economic strength is believed to now heavily rely on the ability to acquire, manipulate, and exploit information, the transformation in global military affairs (shijie junshi gaige) is seen as a consequence of the introduction of information technology into various areas of military operations. In short, information technologies are now key in both war and peace.

This shift is reflected prominently in the PLA's evolving description of future wars. Its 1990s call to prepare for "local wars under modern, high-technology conditions" made way for newer concern over "local wars under informationized conditions." PLA professional military literature apparently discussed this change in 1999, five years before the new phrasing appeared in a Chinese white paper on national defense. In 2002, it was "officially incorporated into the lexicon of the 'Military Strategic Guidelines for the New Period.'" [51]

Informationized conditions are marked, in part, by the introduction of information technology into various weapons, making them ever more precise and lethal. The networking of weapons with one another and with sensors allows for higher operational tempos, as night and weather conditions no longer constrain military forces to the same extent as in the past. But informationized warfare goes beyond the incorporation of information technology into individual weapons, or even into broader systems.

With the steady proliferation of information technologies, conflicts are no longer determined by platform-versus-platform performance, or even by system-against-system (xitong) factors. Rather, conflicts are now clashes between systems-of-systems (tixi), which emerge through the integration of information flows that themselves are generated by the incorporation of information technology into every facet of military activities (e.g., logistics, intelligence collection and exploitation, transportation, etc.). [52]

Key to the struggle between systems-of-systems is the ability to affect that information flow: the ability to secure information dominance (zhi xinxi quan). This entails "an emphasis on the use of command decision-making to form and shape the entire whole." [53] Accordingly, informationized warfare emphasizes the incorporation of advanced information technology not only into command-and-control capacity as an integral part of generating additional combat power, but also into various combat, combat support, and combat service support functions.

Importance of Space Dominance

The growing role of information in modern warfare, to the point where it is also a weapon, has further elevated the importance of space in the context of "informationized warfare." Support from space-based systems is essential for land, sea, and air operations. The information derived from reconnaissance and surveillance satellites, navigation satellites, meteorological satellites, and communications satellites are the enablers for "non-contact," "non-linear," and "non-symmetric" warfare. A position of advantage in space bestows benefits that eclipse all other forms of military "high ground."

In "local wars under informationized conditions," it is therefore essential to secure space dominance (zhi tianquan): the ability to establish control over specific areas of outer space at specific times. The objective is to establish an advantage in outer space, ensuring one's own freedom of action in space while denying an opponent the same. [54] As the second edition of the Chinese Military Encyclopedia goes on to note, the side that has the advantage in space will be able to constrain operational activities on land, sea, and air battlefields:

> Space dominance will be a vital factor in securing air dominance, maritime dominance, and electromagnetic dominance. It will directly affect the course and outcome of wars. [55]

Given the importance of establishing space ", some Chinese analyses conclude that space battles will constitute the initial operational activities in future informationized conflicts.[56]

Such battles may take several forms:[57]

- Space information operations (taikong xinxi zuozhan). This approach directly assails the key point of space systems: their information systems. Such operations will employ space electronic warfare and space computer network warfare to disrupt enemy space platforms, including electronic and computer systems. Such "soft" methods have the added advantage that they may be harder to detect and defend against.

- Space anti-satellite operations (taikong fanweixing zuozhan). This approach will destroy enemy space information systems, whether through space or ground weapons, space mines, or directed-energy weapons. Physical destruction is arguably the most effective means of attaining space dominance, but it has potential diplomatic repercussions.

Nonetheless, the PRC has continued to display interest in technologies that could be employed in a "hard" kill fashion. In 2013, China conducted an anti-missile test closely resembling a 2010 Chinese test that the U.S. Department of Defense then described as "two geographically separated missile launch events with an exo-atmospheric collision."[58] Such a system clearly also has ASAT potential. Similarly, China has experimented with small satellites in ways that may reflect an anti-satellite role. In 2010, China became only the second nation to rendezvous two satellites, a capability that has military as well as civil applications.[59] More recently, the Chinese satellites Shiyan-7, Chuangxin-3, and Shijian-7 engaged in a series of maneuvers that raised concerns among U.S. analysts.[60]

In addition to offensive operations, space defensive operations (kongjian fangyu zuozhan) will be necessary for countries to preserve their space systems.[61] Possible measures include camouflage and deception, hardening, satellite movement and dispersal, autonomous systems, and on-orbit reserves, including deployments to higher orbits. Because space is a holistic structure, terrestrial assets such as launch sites, telemetry/tracking and control systems (TT&C), and mission control facilities require protection, primarily through active and passive defenses and mobility. Finally, data and TT&C links require protection against potential strikes, including cyber attacks.

Deterrence and Diplomacy in Space

For China, the ability to establish space dominance does not solely reside in direct wartime operations; influencing adversary perceptions is an essential element of the Chinese approach. In this regard, the Chinese concept of deterrence (weishe) is key. Whereas Western analysts equate "deterrence" solely with dissuasion, China sees it as also embodying coercion. Thus, a demonstrated ability to threaten an adversary's space systems (such as through ASAT tests, military space exercises, and war games) may influence an adversary's decision-making calculus.

By contrast, China does not appear to have much interest in space confidence-building measures. While China and Russia have regularly tabled proposals on space arms control, they are often transparently self-serving (China's direct-ascent ASAT, for example, would not be affected at all by their proposals). U.S. efforts to engage China in discussions of space confidence-building measures at an array of bilateral fora, including the Defense Consultative Talks and the Strategic and Economic Dialogues, have been consistently rebuffed.

Conclusions

Since 2013, Chinese military modernization efforts have continued apace, sustained by further double-digit increases in China's defense budget. Its focuses have included expansion of cyber-warfare capabilities and tests of new ASAT systems, including a new capability apparently designed to intercept satellites in geosynchronous orbit, an area of space hitherto thought to be safe from earth-based attack. China's test signals that many key communications and strategic warning satellites will be vulnerable, and it again demonstrates Beijing's serious interest in an ability to establish space dominance.

DIMENSIONS OF CRISIS STABILITY IN SPACE

The Space Crisis Stability Challenge

The stage is now set to examine crisis stability in space, which faces its current fundamental challenge in the ease and ultimate preferability of launching a disabling first strike against the space assets of a space peer or near-peer over retaliating against an adversary first strike, absent other considerations (which will be discussed shortly). This is the essence of crisis instability, when pre-emption carries far greater benefits than retaliation. As China in particular becomes more powerful in space, these issues become more worrisome. The future of crisis stability in space will depend on how space architectures and perceptions shape the strategic landscape, but the trends are not encouraging and pose serious questions for U.S. security and for crisis stability more generally.

Beyond certain *de minimis* space offense activities like jamming individual satellites, the current absence of a truly resilient U.S. space architecture, and the many ways that U.S. space assets multiply the effectiveness of both U.S. weapons and decision-making, suggest that there will be strong incentives in a serious crisis for China to initiate and rapidly escalate attacks against U.S. space infrastructure. While China may not wish to initiate such attacks, it could feel compelled to strike in space before the United States does, rather than risk the far more dangerous alternative of striking second. Of course, China also possesses strong disincentives for attacking (e.g., the potential to endure grievous economic damage), which is why neither country would likely engage in more than modest forms of space offense (e.g., space asset jamming) in situations short of a serious crisis. In the intense political heat of a serious crisis, it will be important for the United States to recognize China's incentives and disincentives to strike first in space, and through advance preparation to be able to dissuade Beijing from potentially taking fateful steps in this domain.

Specific incentives for the United States to attack first in space would include the possibility of taking out Chinese space assets that enable China to fire anti-ship ballistic missiles (ASBMs) at U.S. aircraft carriers, long before the U.S. ships approach China's

mainland. Meanwhile, China's incentives to attack first in space would include the potential elimination of U.S. satellites that could detect such ASBM launches, as well as other space assets that would provide the United States with key intelligence on Chinese forces.

Such first-strike incentives would complicate efforts to manage or control escalation in space, as well as leadership efforts in both countries to avert a larger war. The space domain's novelty and a relative lack of conflict experience there—particularly in China's case—would likely diminish prospects for stability and increase the chances for unstable escalation in a crisis. (China also faces broader difficulty in handling crises, such as the 2001 EP-3 aircraft incident, as a result of its relative crisis inexperience.[62])

Without much greater space asset survivability or resilience, peer adversaries in a serious crisis would each possess significant incentives to strike first, when each has its full panoply of functional space assets and an ability to place its forces, space and non-space alike, at maximum readiness. Any second strike would take place from a weakened position due not just to the loss of space assets themselves, but also to the reduced effectiveness of forces that depend on those space assets for information.

While developing advanced counter-space capabilities requires a sophisticated technological base, doing so is not unduly expensive, at least in comparison to the cost of other major offensive capabilities that major powers seek. Herein lies another important concern for stability in space: for China and Russia, credible ASAT and offensive space control capabilities are currently of reasonable technical challenge and cost to develop for the substantial military benefits they can potentially provide. Anytime a relatively modest defense investment can create disproportionate danger to an adversary, there is an inherent risk of strategic instability. Thus from a narrow military perspective, there are ample strategic incentives for technologically advanced countries with important security issues to develop and deploy offensive space capabilities. The sudden loss of SEIS for military forces could easily be strategic in its impact, and the ability to credibly threaten an adversary's SEIS would provide significant leverage in a crisis. A country may still have great leverage without such offensive space capabilities, but it is difficult to argue that such space capabilities would not enhance that leverage, especially if one side had them and the other did not.

As we saw earlier, Chinese military writings suggest that China would have strong incentives to preempt and escalate in space if it considered war with the United States to be inevitable, or if low levels of terrestrial conflict were about to become much more substantial. This mindset could be reinforced if China perceived itself as militarily inferior to the United States overall, and thus at risk of a U.S. first strike placing it at great disadvantage. One Chinese analyst notes explained this position:

> If a side does not seize the initiative before a war starts, once the war erupts, then it will be even more passive.[63]

If we assume that the United States benefits more than China from space capabilities, especially in the western Pacific, then China would have clear incentives to preempt in space, while it still could. Beijing's alternative, after all, would be to wait until the United States achieved major conflict objectives through its overall military advantages, likely degrading Chinese space and other military capabilities along the way. Given that choice, China presumably would want to limit the military effectiveness of U.S. aircraft carriers in the western Pacific using its anti-carrier ballistic missiles, which depend highly on targeting and other information that China receives from military satellites. Those Chinese satellites would be high-priority targets for the United States should serious hostilities break out, further raising pressure on the PLA to escalate first in space. For these reasons, China would likely be tempted to preempt in a crisis or escalate rapidly if a certain threshold were crossed in early hostilities, though neither of these predictions is absolute.

Short time-frames are inherent in crisis scenarios and lend themselves to worst-case interpretations of an adversary's actions. Indeed, the advantages of space attacks and especially of cyber attacks appear likely to diminish shortly after an initial offensive, as the attacked country rapidly "buttons up" its systems and moves into a major system protection mode. The incentive, then, is to hit first and hit hard to maximize attack effectiveness, an escalation incentive that further poisons the early build-up of a crisis. This is a recipe for miscalculation and misunderstanding. In addition, while an action like a kinetic attack (i.e., one involving the physical attack and destruction of a satellite) in space is visible, a number of other space actions would likely be undetected by the attacked side, or at least not easily attributable. One senior Department of Defense official made this case:

> If there is an attack against a space asset, it isn't visible. You can't watch it on CNN, and unless you're directly affected by the capability that the space assets provide, you're probably completely oblivious that the attack happened.[64]

Stability issues chiefly arise with adversaries in possession of significant counter-space capabilities. If localized conflict with a space near-peer is already underway, then the United States should consider the use of tactical, non-strategic, and preferably reversible offensive space capabilities, but only in a selective battlefield manner where there are clear benefits that substantially exceed those obtainable by alternative force options, and where indirect collateral effects are understood and deemed insignificant. (The opponent's decisions would likely incorporate at least some elements of this same calculus.) Again, the key is to determine whether or not the benefits of employing offensive space capabilities substantially outweigh the costs, where each are assessed in a broad framework of U.S. security interests. Crisis stability in space is just one subset of the larger challenge of maintaining crisis stability over all the major domains and across other elements of national power. Vulnerability in one narrow area, such as space, could collapse the broader structure of deterrence more generally if a militarily inferior adversary saw space as its only chance to turn its prospects around, weaken its adversary's prospects, and prevail.

Another dimension to potential instability in space is the "sorcerer's apprentice" problem. Very little experience or history for crisis behavior in space is available to guide senior military leaders, much less the senior political officials to whom military leaders report in the United States, China, and Russia. While war games can provide some relevant background, it is notoriously difficult to get senior military leaders and especially political leaders to participate meaningfully in such exercises. And to date, no country has any significant experience in space conflict, resulting in a separate risk of escalation from the mutual unfamiliarity with the dangers involved. Aggravating this inexperience problem is the fact that there are no international understandings on the uses of the space and cyber domains, where miscommunication and misunderstanding can too easily lead to crisis and rapidly escalating conflict.

The Strategic Landscape of Space

Space is largely an offense-dominant domain. Certain defenses are possible against some offensive threats, and there is likely an ill-defined threshold below which space- and ground-based segments of space infrastructure can be defended, but effective defenses against a determined and sophisticated space peer seem unlikely—at least for a number of years. Unless a country develops effective offensive space capabilities that do not themselves depend too greatly upon space assets, the vulnerability of existing offensive space capabilities suggests the potential for greater instability.

Despite understanding the likely direct effects of offensive strategic nuclear forces, large uncertainties persist about the probable collateral and indirect effects of any large-scale use of nuclear weapons, though these side effects were mostly under-appreciated during the Cold War. The blast, fire, and direct radiation effects of nuclear arms were recognized from the very beginning, their radioactive fallout effects somewhat later, and their climatological and other effects only much later. Similar uncertainties characterize the prospective large-scale use of offensive counter-space capabilities, and the indirect effects of an all-out strategic cyber-war are virtually incalculable. In this regard, a strategic space or cyber war against a peer or near-peer opponent may be somewhat like a strike involving highly virulent biological weapons, in that any such attack could cause nearly as much damage to an aggressor as an adversary. Uncertainty regarding the collateral effects of such strikes prompts a level of self-restraint among potential users, who act from a mixture of rational calculation and adversary influence. Such uncertainty appears to be an intrinsic feature of the strategic cyber environment and to some extent the strategic space environment, but the resulting deterrent and stability effects in either domain are difficult to gauge. While it may have a deterrent effect against escalation, a country may still minimize such uncertainties and act regardless, especially if it saw itself near defeat in other domains.

Electronic warfare has a relatively long history in the annals of modern conflict, where radar jamming and other steps have often appeared in tactical situations; this state of affairs is unlikely to change. Iran and others in the Middle East, for example, have used satellite jamming technology to block Eutelsat television transmissions as early as 2009. At a purely tactical level, therefore, it seems highly likely that small-scale use of offensive space capabilities of this sort will occur. Such use would not necessarily be destabilizing, though it may not always be wise. Where major space powers are involved, key factors will be the type and scale of a possible target. Indeed, scale is a fundamental issue for assessing crisis stability in space. The threat of an unstable escalation of space attacks is real during a crisis and jamming one or two GPS satellites in isolation would carry risks, but such action seems unlikely to precipitate an all-out space war, given the longstanding role that electronic warfare has played in conflict. Attacking U.S. intelligence-gathering and launch detection satellites would be another matter. Between these extremes is likely a line—ill-defined, unpredictable, and shifting with circumstances—dividing steps that are modestly threatening to stability from those that are highly destabilizing and escalatory.

One of the subtle but important changes in U.S. space operations over the last 30 years has been the continued integration of U.S. space capabilities that once had

been almost exclusively tasked with strategic missions (e.g., electronic intelligence, communications intelligence, and infrared missile warning) into operational/tactical war-fighting missions, where they now directly support war-fighting and thus become conventional conflict targets. But their strategic nuclear roles have not gone away. This means that, for example, China could attack these satellites for purely conventional war-fighting purposes, yet the United States could see this as an attempt to weaken its strategic nuclear capabilities, thus fomenting major escalation, further heightening crisis instability before such attacks, and rapidly propelling the conflict up the escalation ladder during and after such attacks.

It appears safe to say that a very modest use of counter-space capabilities during a crisis or in the early stages of a conflict would not trigger all-out attacks against opposing space infrastructures, though it would certainly encourage the other side to take compensating defensive and tit-for-tat measures as well as put additional offensive capabilities on a higher alert status. Thus, while not escalatory in themselves, these low-level measures would at least provide more fertile ground for escalation to take place.

One of the crucial crisis stability questions arises just after such measures, in the form of the "slippery slope" of crisis instability. Given the lack of clear red lines on the space escalation ladder, coupled with the complex interaction between space and other domains, there will always be a temptation for at least modest escalation, though with the belief and intent that the apparently modest step would not lead to much greater escalation. But the strategic landscape of space is new and largely uncharted; even modest escalation beyond some low point could result in rapid, mutually undesired escalation through unappreciated mechanisms. As if this were not enough, the landscape of the space and cyber domains is evolving far more rapidly than the nuclear domain did in its early years, meaning that effective strategies at a particular time may become ineffective within a few years. In the Cold War, ironically, the United States and the Soviet Union largely came to understand that any use of nuclear weapons would lead to all-out nuclear war, minimizing temptations to use even small nuclear weapons for tactical purposes. In space—or cyber space for that matter—adversaries may learn how much escalation is too much only after it is too late to stop.

For most of the nuclear era, the United States and the Soviet Union each had a good idea of the strategic offensive and defensive forces the other had deployed, and the effects those forces could inflict on different classes of targets. This is much less true

for space offensive forces and defenses, and far less true still for cyber offenses and defenses. Space- and cyber- situational awareness are nowhere near as characteristic of these new domains as they were for strategic nuclear weapons in the late Cold War. This missing ability to gather solid information on the types and status of deployed capabilities is one of the most significant features of space, and particularly of cyberspace. This means that uncertainty, worst-case thinking, and bluffs will likely figure prominently into crises in space and cyberspace, to a far greater extent than in the nuclear domain.

Alliance structures are another major factor affecting space stability and space deterrence, especially in a crisis. During the Cold War, the United States largely shouldered the nuclear-related costs of European security. With the exception of Britain and France, contributions in the nuclear domain by Washington's NATO allies were limited chiefly to basing rights, some dual-capable aircraft, and moral support; these were valuable contributions to be sure, but the United States nonetheless did the heavy lifting from a burden-sharing perspective. Indeed, the unspoken hope of the United States' European allies in the Cold War was for any nuclear war to quickly escalate to the strategic nuclear level and unfold "over the heads" of Europe, largely sparing the continent while inflicting most damage on Soviet and U.S. territories.

The space and cyber domains present a substantially different picture. In a crisis, China, for example, would face not only the United States, but also the rest of NATO as well as Japan, South Korea, Taiwan, and others whose combined economic powers dwarf even China's substantial economy. While China has no major allies and a recent track record of intimidating its neighbors, trade and communications links connect those other economies to an extent that any major Chinese strategic space and/or cyber attack against the United States would effectively be an aggression of equal magnitude against most other major economic powers, many of which have committed to defend the United States if attacked. And with the exception of some highly specialized military and intelligence satellites, U.S. allies and others are quite economically dependent on U.S. space infrastructure. Because the United States also depends on non-U.S. commercial space infrastructure, China also would need to attack numerous non-U.S. satellites to ensure that the U.S. cannot simply move its priority communications to this non-U.S. space infrastructure.

Targeting many non-U.S. space assets in a potential space attack against the United States is an exceptionally tall geostrategic order for China, representing an easily overlooked dimension of U.S. international strength. Making matters worse, China

itself uses this transnational civilian space infrastructure and would suffer from its degradation or loss. The economic havoc that a major Chinese space infrastructure attack could cause to the United States, Europe, Japan, and elsewhere would also deliver a body blow to the Chinese economy, which is highly dependent upon healthy and functioning foreign markets for its continued prosperity. Given China's major export dependence on these markets, and its dependence upon them for key raw material and high technology imports, it is highly likely that China would suffer major economic devastation even in a best-case scenario—hardly a healthy outcome for the Chinese Communist Party (CCP). Further, China would then need to contend with the military and economic retaliation of tens of economically powerful countries. PLA theorists and planners may not keep these factors foremost in their minds in their writings, but it is difficult to believe that the members of the CCP Politburo Standing Committee would not be fully aware of, and heavily influenced by, these geopolitical realities in their crisis decision-making. It would be a serious mistake to underestimate the deterrent effect of this disparity and the advantage it represents to the United States and its allies. This major U.S. advantage is too easily overlooked in assessing the respective military strengths and weaknesses of the United States, China, Russia, and others.

Space probably shares more similarities with the cyber domain than the nuclear domain, though important commonalities exist among all three. War, crises, and the general workings of deterrence seem much less likely to begin, or end, in space. Space, like cyberspace, is likeliest to be a single dimension for larger threats or conflicts that span multiple domains, rather than a unique locus of military operations and attacks.

The evolving space security environment can and will affect crisis stability dynamics. The space environment of 2025 or 2030 probably will be different than the space environment of 2015, unlike the nuclear environment, which changes much more slowly. (Likewise, the rapidly changing cyber environment will certainly be substantially different in ten to fifteen years.) As a result, space dynamics may undermine today's understanding of crisis and strategic stability in space. The ability of nuclear weapons to inflict horrendous damage has established a clear and enduring taboo against their use; crossing the nuclear threshold has significant, immediately recognizable implications. Moreover, experts generally could determine motives for a nuclear attack through the weapon (whether it is strategic or tactical) and its target (whether it is counterforce or counter-value). This type of discernment is far more complicated in space, where no clear, mutual understanding exists concerning the value of particular targets or the implications of employing particular space weapons. In addition,

space weapons can inflict far more discrete and "granulated" damage than nuclear weapons, lowering the threshold for possible space offense use by senior leaders and making further escalation superficially more appealing. (This excludes the possibility of the pre-conflict space environment becoming so dense with debris that additional debris from a major space conflict would trigger a self-sustaining chain reaction of collisions known as the Kessler Syndrome, making space far more dangerous for most satellites.[65])

To address these factors in a space context:

- There is no taboo against the use of many counter-space systems. The threshold for using temporary and reversible counter-space capabilities, such as electronic interference, is largely untested and likely much lower. In addition, the number of actors with such capabilities is unacceptably high; even non-state actors can jam satellite communications.

- Temporary and reversible weapons appear to be less escalatory than kinetic kill weapons, such as those tested by the United States and the Soviet Union during the Cold War and by China more recently. The effects of kinetic kill vehicles weapons are insidious; their short-term impact may be quite modest, but they generate space debris that indiscriminately threatens all satellites for decades into the future.

- Weapon survivability is also crucial to consider. As noted earlier, space is an offense-dominant domain, creating first-strike instability. The offense-dominant nature of space has implications for both peaceful satellites and space-based weapons. Space-based weapons would be quite vulnerable to attack if their presence were known to an adversary, and such assets would thus be extraordinarily destabilizing, confronting both sides with overwhelming incentives to strike first in a crisis. Weapons unknown to the other side would not be destabilizing, but ironically, the use of previously unknown weapons would likely strongly encourage the attacked country to escalate almost at once. As we will discuss later, the vulnerability of all space-based weapons highlights the absence of any space-based equivalent to the highly secure and survivable sea-based forces of the nuclear weapons domain.

Any space power presumably would seek to reduce the vulnerability of its space assets, whether they are in space or on the ground. A powerful but highly vulnerable

space architecture would place its operator in a "use-or-lose" position against a space adversary in any serious crisis: if the first power held back, it could lose its space assets to a first strike by the adversary, which would retain most of its own space assets. A power in possession of a vulnerable offensive space capability would thus face significant pressure to attack first in a serious crisis, absent other considerations. This situation reflects what Herman Kahn noted over half a century ago: "A nation is most likely to go to war when it believes it is less risky not to go to war."[66]

The general solution to this type of instability problem is to reduce the space architecture's fragility, thereby reducing the advantage an adversary would gain from attacking first. Transferring some capabilities from space to earth would help to reduce dependence on space, but some functions must take place in space. A global power like the United States will not escape its significant reliance on space to project power; over-the-horizon targeting of weapons systems relies on space, and the assessment of damage from a distance (an under-appreciated element of military operations) often does as well. Resilient space systems with significantly greater resistance to attack and system failure remain distant goals for both China and the United States.

As Chinese military dependence on space grows going forward, and particularly as China increasingly requires monitoring capabilities much farther from its shores, the advantages of restraint in space should become clear to Beijing, which will not want to lose its space assets to U.S. retaliation. This understanding will be sufficient to maintain space stability in peacetime, but such peacetime restraint could well crumble in a serious crisis if the space capability vulnerability issue is not first resolved. In such a case, both sides would face a "use-or-lose" situation, producing space instability that the adversaries would have to manage through a combination of diplomatic and technological steps. Accomplishing these mitigating actions would be a major challenge and require significant cooperation, dialogue, and technological advances among the major space powers—or, at a minimum, a willingness to tolerate higher levels of risk.

A fundamental challenge in a crisis is to balance prudent preparation for conflict—in part for the reassurance of allies—against the risk that an adversary will misinterpret such action as a sign of an imminent first strike. Following this exquisitely fine line will be fraught with risk and danger, yet refusing to prepare for a possible attack is an unacceptable alternative. While quick preparations for conflict would generally be more destabilizing than slower preparations, the latter approach would carry its own risks. Communication and dialogue would be essential at all stages of a space

crisis, and any such interaction would be easier to conduct through channels that had been in place and active prior to the start of the crisis.

In short, the strategic landscape of space has some similarities to the conventional and nuclear domains, but it is substantially different and not well understood in important respects. The vulnerability of space assets is a major and growing concern that would create incentives during a serious crisis for a space power to strike first against its adversary's space assets. Beyond certain ill-defined lower levels of political and military tension, there appear to be no benefits to gradual escalation of space conflict and major benefits to quick space escalation against an adversary. Complicating this picture still further are the world's shared inexperience in space offense and the highly interconnected nature of world economies, which make the collateral effects of any major space conflict largely unknown and perhaps unknowable. Alliances and friendships appear to provide the United States with major, under-appreciated peacetime and crisis advantages that China does not enjoy.

Comparing the Four Domains

Comparing the different domains of conflict can reveal deeper lessons about crisis stability and instability. This report will use four domains for this purpose:

- Nuclear
- Space
- Cyber
- Conventional

These selections are somewhat arbitrary; for example, the conventional domain could be further broken down into air, land, and sea. This analysis will not separately address the conventional domains, however, because their unique characteristics are less significant than the attributes that distinguish them from the other three domains.

The following table (Table 1) is a rough sketch comparing and contrasting the space, cyber, nuclear, and conventional conflict domains according to several strategic planning considerations. While hardly authoritative, the table suggests that the variation across domains is pronounced, and that lessons learned from one domain should not be applied to other domains without careful review and analysis.

While the table's judgments of the space and cyber domains may appear particularly debatable, that fact merely underscores the emerging strategic competition in these two areas, where the strategic landscape is nowhere near as well defined as in the conventional and even nuclear domains. This table should not be considered definitive, but rather as a starting point to provoke the reader's own ideas about similarities and differences among the four domains.

Table 1. Strategic Domain Comparison[67]

Feature	Nuclear	Space	Cyber	Conventional
Limited use is escalatory?	YES	NO, but…	NO, but…	NO
Major benefit to first use?	MODEST	YES	YES	MODEST
Knowledge of adversary arsenal?	YES	YES, but…	NO	YES
Understand effects?	YES	?	NO	YES
Are there cascading effects?	YES	LIKELY	YES	MODEST
Rate of environment change	MODEST	HIGH	VERY HIGH	MODEST
Arsenal vulnerability	MODEST	?	?	MODEST
Secure reserve force?	YES	?	?	MODEST
Role of uncertainty?	MODEST	HIGH	VERY HIGH	MODEST
Countries have experience	U.S. >> China	Limited	MODEST	U.S. >> China
Actions attributable?	HIGH	LIMITED	MODEST *but increasing*	HIGH
Offense-dominant?	YES	YES	MIXED	LOW
Economy-enmeshed?	NO	YES	HIGH	LIMITED
Nth country significant?	MODEST	YES	YES	MODEST
Actions monitorable?	YES	MODEST	LIMITED	YES

The table yields one consistent finding: no domain is identical to any other. Experience in one domain, then, is not a fully reliable guide to behavior and crisis decision-making in another. This does not mean that other domains' features are irrelevant, only that great care is necessary when drawing analogies between domains.

Several other conclusions can be drawn from this table. The space and cyber domains share the greatest relative similarity, due in part to the relative lack of experience in either domain that necessarily places limits on our understanding. The nuclear and conventional domains appear nearly as similar, surprisingly enough, though there are highly significant differences in their potential to produce escalation through limited use and in the security of their reserve forces. The United States has more experience than China with regard to nuclear decision-making and domain familiarity, but the United States fortunately has no actual warfare experience with a nuclear-armed adversary in this domain. With thousands of years of land- and sea-based conflict experience and nearly a century of air combat history, all nations certainly have combat experience to draw upon in conventional domains, though some more than others.

This chart also illustrates why the strategic landscapes of space, and of cyberspace, are so uncertain and potentially dangerous. The space and cyber domains are changing much more rapidly than the conventional and nuclear domains, creating far less certain environments in which potential adversaries may employ force. Experiences in these domains that may initially guide sound decision-making will retain some relevance with time, but they will grow outdated faster than comparable past experiences in the conventional and nuclear domains. Of the space domain's distinguishing characteristics, its feature most significant to crisis stability may be the substantial benefit of first use in space when conflict seems inevitable. As noted earlier, beyond low-level interference with space assets, launching a significant first strike against an adversary's space assets appears far preferable to allowing that adversary to strike first. This attribute of space not only strongly suggests a relatively high level of crisis instability, but it also suggests that escalation could proceed rapidly. (This finding assumes that technology for providing assured space connectivity does not change substantially in the future.) The cyber domain appears to favor first use as well, though probably not as strongly as the space domain.

One more destabilizing dimension of the space domain is the quite limited potential for many attacks against space assets to take a direct toll in human lives, even when the possible destruction of ground-based space assets is considered. Therefore, political demands for retaliation within the attacked country would likely be far less than for

an attack that ended tens or hundreds of lives. The old military space saw "satellites don't have mothers" is relevant here.

The question remains: At what point does the limited tactical use of counter-space capabilities or cyber weapons take us to a crisis tipping point, where miscalculation, misunderstanding, Murphy's Law, and Mother Nature—these Four M's are the modern-day Four Horsemen of strategic apocalypse—trigger a crisis, a small-scale conflict, or a show of force that escalates into full-scale conflict? This ambiguous threshold is one of the great unknowns, though additional analysis and simulations may dispel at least some of the uncertainty. The United States should approach such exercises as urgent tasks to strengthen its security.

The United States currently depends on its space capabilities significantly more than China relies on its own space capabilities, giving the United States more to lose from space conflict than China. This disparity will likely decrease as the PLA grows more dependent upon its space capabilities, but it will still persist some years into the future.

Deterrence, and Differential Deterrence, in Space

Deterrence is a fact of life in every military domain, but it assumes different forms that reflect each domain's specific characteristics. To better understand how deterrence operates in the space domain, it is important to recall a point repeated throughout this report: any situation or crisis in space is highly unlikely to be confined to the space domain alone, and it may well not originate in space. Rather, it will probably involve the other domains to a greater or lesser extent, and that involvement will influence how deterrence operates in space.

A fundamental question in this regard is the nature of an adversary's offensive space policy and doctrine. While this issue is most relevant to the U.S.-China relationship, it would apply to other countries that may develop space weapons. In the case of the United States and China, the question becomes whether each country generally operates from a space deterrence strategy or a space war-fighting strategy. This question is complicated by the fact that a well-reasoned space war plan, supported by a suitable space architecture, is itself a strong deterrent. Conversations with Chinese experts in Track 1.5, Track 2, and other fora[68] suggest that both sides believe they are operating under a space deterrence strategy; certainly neither side is actively looking for space conflict, given the stakes involved. On the other hand, neither side is confident that the other is only pursuing space deterrence, or that in a crisis the adversary would not pursue space war-fighting options if deterrence failed.

It is not difficult to envision the execution of low-level space offenses, on the order of jamming a satellite, during a crisis or conflict. While such action will not please the affected country, it also probably will not lead, ipso facto, to Armageddon in the manner that even low-level nuclear weapons use may conceivably accomplish. As long as the United States maintains credible conventional forces, nuclear forces, and cyber capabilities, it should have sufficient forces to deter most forms of aggression in space. Accordingly, the United States will not require an offensive space capability to deter an adversary in space as long as it is perceived as willing to respond decisively in another domain to adversary space offense. U.S. policymakers likely will not need offensive space assets to achieve overall deterrence, but they may want such assets to enhance the country's overall deterrent capability. In addition, they may want or need capabilities for space war-fighting because deterrence may function less effectively against lower-level adversary space attacks, especially those of a reversible nature. This is stated without passing judgment on whether or not the development of such capabilities is advisable for the United States. This presupposes the credibility of out-of-domain threats, but this assumption seems reasonable in a risk-averse crisis atmosphere.

While explicit U.S. offensive space capabilities may not be needed, the question remains: would such capabilities be desirable to enhance deterrence and crisis stability, especially given that China appears to have such offensive capabilities? Some observers believe not; they argue that residual U.S. offensive space capabilities from jamming and limited ASAT capabilities inherent to national ballistic missile defense systems should suffice. Others believe that pursuing offensive capabilities beyond such residual capabilities would benefit the United States, given China's actions in this arena, as part of a space deterrence strategy. To do otherwise, in their view, would cede an important domain of military activity to a potential adversary. In addition, the absence of more offensive space options may force the United States to respond to a nonlethal adversary space attack with non-space actions that would produce casualties, placing Washington in the geopolitically awkward position of spilling the first blood in a conflict. Few provocations are as effective in influencing public opinion as waving a bloody shirt; Jordan's military reaction in early 2015 to the execution of a Jordanian pilot by the Islamic group ISIS joins a vast company of similar reactions in history, the domestic political force of which should not be underestimated. Cyber offense against space assets could provide nonlethal retaliatory capabilities to address this problem, though it may not be advisable to rely too much on forces in the poorly understood cyber domain to maintain deterrence in a crisis.

It appears possible to justify at least some offensive U.S. space capability on purely deterrence grounds, at a minimum to deny potential U.S. adversaries a "free ride" where space offense is concerned. As noted above, direct action in space does not always lead to direct casualties on the earth, whereas most non-space retaliatory actions, such as attacking launch sites, involve casualties and direct incursions in an opponent's homeland. Such non-space responses would raise the potential for emotion-driven additional escalation, thereby making them less feasible options for the United States to pursue during a crisis. The extent and purpose of a prospective offensive U.S. space capability both remain unclear; these are issues beyond the scope of this report, but they will need to be addressed and must not be overlooked.

While the rules of strategic nuclear deterrence and stability do not directly translate into the space domain, much less the cyber domain, nuclear principles still remain relevant; they simply take new forms, with behaviors that are sometimes starkly different. One clear example concerns the distinction between tactical and strategic offense. In the nuclear domain, any use of nuclear weapons would almost always lead to general nuclear war, as shown in war games. Yet due to electronic warfare's far more limited effects and its longstanding use in past conflicts, the limited tactical[69] use of space offense in the early stages of a conflict, or even in the late stages of a crisis, is much less likely to trigger full-scale space warfare, much less a nuclear war or even a major non-nuclear war. Miscalculation in tactical space conflicts appears relatively unlikely, as the United States already has some real-world experience to draw upon in handling adversary attempts to jam its satellites in tactical situations, as well as in more generalized electronic warfare. This experience does not exist, however, for much broader uses of offensive space capabilities. Because neither the United States nor any of its potential adversaries have any experience in waging a strategic space conflict, accurate assessments of how such a conflict would unfold simply are not possible. Complicating this problem further, battle damage assessments from space attacks can be far less certain than in conventional conflict, especially for attacks with temporary and reversible effects.

Smaller space powers ironically enjoy greater leeway in using their limited offensive counter-space capabilities than a major power, like the United States or China, because smaller powers cannot credibly threaten a major strategic space offensive, whereas a major power can. Jamming several U.S. satellites, for example, would be perceived as a more threatening action if committed by China than Iran, because China possesses far greater offensive counter-space potential than Iran and would likely have more threatening objectives in doing the jamming. Thus, the degree to which an action is destabilizing during a crisis depends on what country carries out the action and that power's perceived objectives.

If the United States perceives China to be its prime space adversary, U.S. policy will likely seek to undermine any Chinese determination that China would benefit from attacking the United States in space or any other domain. While a U.S. offensive space capability may marginally influence Chinese thinking on this matter, its effect probably would not be decisive.

In considering how deterrence might function in space, it would be a mistake to treat all space assets as one undifferentiated category. Likewise, it is important to differentiate among orbits, given, for example, that there are more options to attack quickly in low earth orbit (a few hundred miles above sea level) than in geosynchronous orbit (roughly 22,200 miles above sea level). Each class of space assets has a different value to both attacker and defender, and each as a result has "differential deterrence" and war-fighting implications. An attack against U.S. space assets directly related to strategic nuclear forces clearly would have different implications than an attack against a civilian communications satellite.

By the same logic, a reversible attack against a space asset should not have the same implications as an irreversible attack against the same asset. However, this proposition assumes that the operator of the attacked asset could differentiate between the two types of attack, a capability that would require satellites to have far more sophisticated on-board self-check features than exist currently. An aggressor's assets may further confuse efforts by an attacked country to discern the nature of a strike: the high-fidelity space situational awareness capabilities that an attacker would require to enable and confirm the effectiveness of reversible attacks would also increase the effectiveness of irreversible attacks. In addition, while reversible attacks may appear less destabilizing, they lower the deterrence threshold for conducting such attacks, making the transition from crisis to conflict at least marginally more likely. Differential deterrence appears to be intrinsic to the space domain, based on target value; this principle also appears to apply in the cyber domain.

One "Crimson Line"

In this context, it is important to highlight the special status that should be accorded to nuclear force-supporting space infrastructure. Possibilities for misunderstanding exist throughout the strategic landscape of space, but in this area there should be no ambiguity: under no circumstances should any country take action that could

be interpreted as threatening to weaken, attack, or destroy another country's nuclear-supporting space infrastructure. This should not just be a "red line," but a "crimson line": a universally recognized, crystal-clear threshold beyond which any aggression would lead to substantial, and potentially grave, escalation of conflict that may even move into the nuclear realm. Some in China have speculated that an isolated attack on an individual launch detection satellite, potentially within the Defense Support Program (DSP) or the Space-Based Infrared System (SBIRS), could be stabilizing if it signaled that the United States is approaching a strategic red line for China. While China can be expected to signal that another nation is closing in on a key red line, attacking a launch detection satellite would be an extraordinarily bad way to do so, as this author and others have expressed in dialogue with Chinese counterparts.

If at least some offensive U.S. space capability were deemed useful, at least ten characteristics would be desirable for this capability, depending in part on the future architectures of China and Russia:

1. *Largely survivable against an adversary first strike.* If achievable, this survivability would serve as an important deterrent to an adversary attack, and it would likewise greatly reduce pressure on the United States itself to attack first in an escalating crisis. By negating the classic problem of "using or losing" offensive space capabilities, this feature would greatly enhance crisis stability. This requirement poses a challenge to many space-based offensive options, whose exposed and predictable orbital positions would render them more vulnerable to attack than land- or sea-based offensive space options.

2. *Temporary and reversible effects capability.* There should be at least a capability, if not a preference, to maintain these effects for extended periods of time, if possible.

3. *Effectiveness.* An offensive space capability must be able to negate the space capabilities of an adversary.

4. *Survivability.* While indefinite survivability would be most desired, any major degradation in capability should be gradual enough to provide sufficient space offense to meet space control and offensive capability requirements.

5. *Resilience.* Similar to survivability, this capability should allow the space offense to absorb attacks yet continue to be able to function in a way that delivers sufficient offensive capability to meet requirements

6. *Little or no collateral damage.* Major debris-producing offensive counter-space capabilities such as kinetic-kill weapons should not be used and should be reviewed for possible international prohibition, given their potential to create very long-lived damage to key orbits.

7. *Seamless connectivity* with conventional, cyber, and other military capabilities.

8. *Flexibility.* The offense must be capable of functioning under a variety of scenarios.

9. *Credibility.* The offense must be perceived as credible to potential adversaries. U.S. allies should likewise perceive credibility, and in a way that reassures them, chiefly through belief that the primary mission of such offense is deterrence.

10. *Maximizes adversary risk aversion.* In delivering offensive effects, U.S. offensive space capability should seek to induce strong risk aversion in potential adversaries through minimum susceptibility to countermeasures, sustained capability, and other features.

It should be noted that many of these characteristics are relevant to cyber weapons, whether for space or other applications.

A capacity to generate reversible effects is generally desirable in space offense, but this attribute is a two-edged sword. Such effects promise to substantially reduce potential damage from battles in space, but they weaken deterrence by making space conflict less damaging and hence more feasible. It is unclear whether or not reversible effects represent a net positive for crisis stability in space. While most decision-makers probably would prefer to have the option available, its drawbacks must not be ignored in considering flexible space options. Offensive space assets whose effects can be increased or reduced—so-called "dial-a-yield" weapons—potentially offer the best of both worlds: they threaten full destruction to maximize deterrence, but they can deliver temporary and reversible effects should deterrence fail and actual use of the weapons come under consideration.

Karl Mueller addresses some of these issues, among others, in the following section.

Six Propositions About Offense, Defense, and Crisis Stability in Space

Karl P. Mueller [70]

Introduction

Crisis stability and deterrence[71] are fundamentally the same in space as in other domains, with which space is intimately connected. Yet space is different in respects that are consequential to crisis management and the formulation of deterrence strategy. This paper briefly examines distinguishing features of space, organized into six interrelated propositions. The first propositions are fairly general in scope, while the later ones more directly address offense and defense issues.

1. Events in space do not happen in a vacuum. [72]

The single most important characteristic of space stability is its high degree of connection with broader stability. In a Sino-U.S. crisis, space would be a relatively small but potentially important part of a larger multidimensional game board.[73]

Space is important to national security due to the effects of space systems on terrestrial crises, conflict, and cooperation. Most of these effects are indirect because as agents of information collection and transmission, satellites primarily function in support roles as force multipliers, enablers of military operations, and critical elements of ISR architectures. Therefore, potential gains from possessing, using, threatening, or destroying a space system generally relate to the implications of such actions for various forms of terrestrial power. (This fact applies even to potential space weapons, which would matter only for their possible effects on terrestrial war-fighting and affairs.) While space systems have intrinsic value as assets that are costly and difficult to replace, it is hard to envision an ASAT attack motivated by a simple desire to break something expensive.

Therefore, in the context of a highly stable Sino-U.S. strategic relationship in which neither side perceived reasons to initiate or even risk terrestrial conflict with the other, even a significant level of instability in space would be very unlikely to lead to war. Conversely, if Beijing or Washington considered war preferable to its other options, deterrence in space would likely fail no matter how stable their structural space relationship, as one side would likely expect to benefit from extending a terrestrial conflict there.[74]

Stability in space still matters, though, due to the considerable potential under certain circumstances for instability in space to negatively affect general stability. An ability to launch a devastating first strike against a rival's satellites would not in itself justify such an attack, but if such an ability made a prospective war appear promising and inexpensive relative to less unattractive alternatives, an adversary's vulnerability in space could be very consequential indeed.

The 1941 attack on Pearl Harbor offers a useful analogy: Japan's perception that it could cripple the U.S. Navy with a surprise strike was not what motivated the country to begin a war with the United States. Rather, once Tokyo had painted itself into a corner where war with the United States and its allies appeared to be the only alternative to a humiliating cessation of its war in China, the U.S. Pacific Fleet's apparent vulnerability played an enormous role in Japan's ill-advised decision to start the Pacific War.

2. As with terrestrial stability, incentives for pre-emption and prevention in space are central concerns.

Deterrence could fail in a Sino-U.S. crisis because of an accident, or conceivably because one side decided that the situation presented a good opportunity to start a war that appeared fundamentally appealing in a broader context. Yet potential incentives for pre-emptive or preventive attack are the greatest concerns even as accidental conflict triggers, and the two concepts therefore merit clear definition.[75]

At the simplest level, pre-emption reflects a belief that striking first is preferable to allowing an adversary to do so, and that executing a first strike provides a sufficiently important advantage to justify the costs and risks associated with going to war. conflict. (Such a sacrifice may appear insignificant in cases where war seems inevitable.) True pre-emption is rare in international politics—statesmen generally are very reluctant to start wars when averting conflict appears to be even a small possibility—but it is easy to imagine a crisis in the western Pacific where one side may deem a first strike to be prudent. Space systems certainly could figure prominently into a state's calculus about first strike advantage, especially if that state is facing the United States or another actor heavily reliant on space services as an element of its power projection capability.

A potential attacker does not have to expect easy victory from a pre-emptive strike, as in the Six-Day War, for pre-emption to look like a smart move. If conflict comes to appear unavoidable and the options narrow to striking first or striking second, the former choice may appear to be the better of two undesirable prospects. Even a relatively weak adversary of the United States may judge pre-emption to be sound

policy; while such action would be desperate, it may well appear worse to let U.S. leaders choose when and how to start a war.

Preventive war is a closely related concept that is often conflated with pre-emption. The difference is that a state launches a preventive war not because striking first is better than striking second, but because fighting now is more attractive than fighting later, typically because it anticipates an unfavorable upcoming shift in the balance of power, vulnerability, alliance patterns, or technological proliferation. Preventive war is less closely associated with crisis stability, but the dynamic can be much the same: if a crisis makes war appear certain or nearly certain, even a defensively minded state may perceive a closing window of military opportunity and decide that the time for war has come.

3. The escalation relationship between space and terrestrial conflict is unclear.
Briefly setting aside the glaring shortcomings of Herman Kahn's "ladder of escalation" metaphor,[76] where would the "Space Warfare" rung on such a ladder be located relative to the more familiar rungs of terrestrial conflict?

Many space policy professionals appear to presume that war in space would represent a major escalatory step from terrestrial conflict. This view certainly makes the notion of "space deterrence" appear reasonable, implying that there should be a decent prospect of keeping a war limited to terrestrial domains. Yet at least since the early 1960s, some space warfare theorists have argued that war in space would be more limited than terrestrial warfare because it would be less lethal; some have even argued on humanitarian grounds for the development of space weapons. Indeed, while a space conflict may cause indirect human casualties by disabling space services such as GPS data and weather imagery, it is reasonable to expect that even a significant war in space would lead to fewer deaths than a modest terrestrial war.

If space warfare appeared to involve a relatively limited application of force, the consequences for stability in space could be profound. Deterrence in space would be more likely to fail in a crisis due to the lower costs of deterrence failure. Likewise, it would prove difficult to keep a sizable terrestrial conflict from spreading to space, as a participating state would have little incentive to exercise restraint in space if it saw an opportunity to gain military advantage through such escalation.

4. Offense and defense are defined differently in space.
In contemplating the relationship between offensive and defensive military capabilities and stability in space, it is worth reviewing basic terminology. In terrestrial warfare and particularly in land warfare, offense and defense are typically understood in territorial terms: offense aims to take territory from an enemy, whereas defense seeks to protect territorial holdings from enemy attacks. Thus, an offensive advantage exists when, given similar resources, it is easier to seize territory than to defend it.

For air power, the pattern is basically consistent. Doctrinally, offensive air operations reach into enemy territory to strike the opponent, while a state's defensive operations seek to protect its own airspace and surface territory from enemy air attack. Bombers and their escorts are offensive, while interceptors and air defenses generally are defensive (though the latter weapons have offensive applications above the tactical level, such as helping to seize enemy territory and then defending it against counterattacks).

However, space is not territorially divisible—at least outside the geosynchronous belt. States do not own the orbital space above their heads. In military space doctrine, attacking enemy satellites is offensive, even if they are collecting intelligence or dropping weapons over one's own country. Likewise, protecting one's own satellites from enemy attack or interference is deemed defensive, even if those satellites are performing a mission that would be considered offensive if conducted by aircraft.[77]

This unique terminology does not necessarily turn the concept of offensive or defensive advantage on its ear with regard to space stability; as in terrestrial warfare, offensive advantage can increase incentives for conflict initiation while defensive advantage can strengthen deterrence. But the definitions of "offense" and "defense" in space make careful consideration of these labels important, because some offensive space capabilities may be stabilizing and some defensive ones quite the opposite. On the other hand, it may be easier to differentiate between offensive and defensive counter-space capabilities than between equivalent capabilities for air power.

5. Space power is offense-dominant at the tactical level.
Satellites are relatively easy to see, they have no terrain to hide behind, and their ability to maneuver is very limited. Consequently, space tends to be an offense-dominant environment. In a world with space weapons, particularly if such weapons could attack each other, striking first would likely offer significant advantages.[78] This aspect of the space environment generally does not favor crisis stability.

However, it is important not to conflate the offense-defense balances at different levels of war. Consider nuclear stability, where submarine-launched ballistic missiles (SLBMs) are tactically offensive but generally strategically defensive,[79] and where long-range surface-to-air missiles may serve either as tactical defenses for home airspace or as an umbrella for an invasion of a neighbor. In the end, it is offensive or defensive advantage at the strategic level that matters in decisions to go to war.

6. At the strategic level, offense-defense dominance in space is more contingent.
In considering offense-defense balance at the level of strategy, the key question is whether a given technological or other development makes it easier or more difficult for an aggressor to attack and seize a neighbor's territory or force it to comply with coercive demands.[80] By this measure, space power does not consistently favor offense or defense and therefore does not consistently enhance or undermine crisis stability. Different space capabilities will have different effects on stability, and many of these implications will vary with factors such as who is participating in a crisis, where the confrontation is taking place, and what is at stake.[81]

The tactical characteristics of satellites still matter—they tend to be relatively vulnerable to attack by enemies who have invested in the necessary counter-space capabilities—but detectability and fragility do not tell the entire story. For example, the significance of a satellite's vulnerability depends not only on how much and for what purpose its users rely on it, but also on how a denial of its utility would affect them. Is there a backup alternative for providing the space service, or a viable option for doing without it? What are the costs of adjusting to the temporary or permanent loss of the system? U.S. military power has become increasingly dependent on space and other states are following suit to varying degrees, but not all of the trend lines consistently point in the same direction.

Other things being equal, space systems tend to be more important for projecting military power over long distances than for defending home territory; expeditionary or long-range strike operations are likely to depend more on satellite communications, satellite navigation, and even space-based weather forecasting than more local operations that benefit from assets such as fiber-optic communication networks. To the extent that this principle holds true, offensive counter-space capabilities may represent a check on offensive military capabilities more generally, inhibiting aggression and conquest. On the other hand, to the extent that the United States serves as a stabilizing force in international affairs through extended deterrence and offshore balancing (a proposition that is certainly open to debate), limitations on the U.S. ability

to perform this function may help to make it safer for regional aggressors to attack their neighbors. Similarly, satellite-based reconnaissance, surveillance, and missile warning capabilities can be useful tools for power projection, but they may have a greater strategic-level impact by restricting opportunities for surprise attacks. (In this regard, their role is something of a macro-level analogue to the defensive advantages that aerial observation provided to combatants on the Western Front in World War I).

The potential for offensive or defensive advantages in space to "cut both ways" does not mean such advantages do not matter to stability in space and more generally. Rather, it underscores the importance of examining their unique roles in particular cases and in relation to other considerations, if we seek to enhance stability in space, and more importantly, beyond it.

U.S. Space Objectives in a Crisis

The overall U.S. goal in space should be, if possible, to shape the space domain to the advantage of the United States and its allies, in ways that are stabilizing and that enhance U.S. and allied security interests. The resulting environment would inherently favor U.S. priorities and threat perceptions, representing a form of parochial stability that China and others would likely find intolerable and seek to undermine. Attaining such parochial stability, much less maintaining it over time, would be a tall order. China would likely resist any U.S. effort to create such an environment, just as the United States would attempt to thwart an effort by China to shape the space domain to its own advantage. Therefore, a secondary U.S. goal should be to account for the space security needs of other space powers, so as to avoid the pursuit of unattainable ideal objectives. U.S. interests are best served by a peaceful (or at least a conflict-free), stable space environment that allows all nations to reap the benefits of space, though an effective U.S. space deterrent should be one component of this environment.

Even space conflict between other countries could well have adverse collateral effects for American security. The United States has an overriding interest in maintaining the safety, survival, and function of its space assets, so that their profound military, civilian, and commercial benefits can remain available to the United States and its allies, especially in a crisis situation. Related issues will gain prominence as other nations join Russia and India in developing space capabilities, particularly if those capabilities incorporate an offensive component. Meanwhile, Japan notably has equipped some of its ships with an SM-3 model similar to one the United States used in 2008 to shoot down an errant U.S. intelligence satellite. If it so desired, Japan could employ

its significant technological wherewithal to engineer a software patch that would endow its existing SM-3 systems with an offensive space capability.

A space environment shaped largely by the United States would not necessarily place China and others at a disadvantage. A properly crafted system of space management should provide ample opportunity for many countries to benefit and prosper. Of course, space more easily functions to the benefit of all parties during peacetime than in a crisis. Indeed, a crisis represents the crucial test of the space system's stability. The international community is most likely to pass this test if it acts during peacetime to codify, respect, and implement various "shock absorbers," such as operating norms, in peacetime space operations.

After crossing a crucial crisis threshold and entering conflict, space adversaries will have major incentives—absent other considerations—to rapidly degrade or destroy the offensive capabilities of their opposition in space, as in other domains. Offensive space capabilities include more than weapons intended to "kill" adversary space assets; they include an entire "kill chain" of systems that enable the delivery of offensive space effects, such as radars and other sensors, command-and-control centers, and communications links. Thus with the onset of conflict, each side will race to "kill the kill chain" of an adversary's space offense, by whatever means are possible and within reason. This process may well include cyber weapons, which generally will be used early and intensively rather than over an extended period of time. Cyber attacks against hostile space assets will tend to be front-loaded, at least by the initial attacker, due to an expectation that the onset of conflict will likely prompt quick defensive steps by the adversary to reduce its cyber vulnerability

Classes of Destabilizing and Stabilizing Actions

The absence of a truly resilient space architecture and the ability of U.S. space assets to act as a "force multiplier" for the United States together ensure that China will have strong incentives in a serious crisis to initiate and rapidly escalate attacks against U.S. space infrastructure. This principle applies to offensive space activities beyond certain de minimis actions such as jamming individual satellites. When one chooses to seriously strike a major adversary, there are powerful incentives to strike very hard. As Machiavelli noted centuries ago, "Never do an enemy a small injury."[82]

This element of potential conflict would complicate efforts to manage or control escalation in space, as well as efforts by the leaders of adversary space powers to avert a larger war. The space domain's novelty, and the relative lack of experience in

space crisis and conflict management, would likely increase prospects for instability and the likelihood of unstable crisis escalation. In addition, China is more generally inexperienced in crisis management, as reflected in its handling of crises such as the 2001 EP-3 aircraft incident.

The following classes of stabilizing and destabilizing actions could help to clarify space crisis stability thinking, potentially serving to inform specific actions considered later in this report.

Operationally Responsive Space

Operationally responsive space (ORS) is a program that seeks to provide some added or replacement capability by launching additional space assets prior to or during a conflict. Such added assets may not be resilient, especially if they share the same fundamental vulnerabilities as the satellites they are augmenting, but the temporary additional capability may be sufficient for the United States to fight effectively until the conflict is resolved. This relatively brute-force approach to the problem of survivable capability has met with a mixed reception in military and other circles. Preparing or launching operationally responsive satellites in a crisis would, at best, send an ambiguous signal that could be interpreted either as a defensive move to increase satellite resilience or as a prelude to an attack, with worst-case thinking probably tending toward the latter. Repositioning satellites also would likely be seen as ambiguous, for similar reasons. No simple means exists to communicate whether an action is being taken defensively or in preparation for an attack, though as a general rule, a rapid deployment could appear more hostile than a drawn-out deployment, and a no-notice deployment could appear more hostile than a deployment accompanied by a public explanation. ORS may become more economically feasible if the United States distributes satellite capabilities across multiple smaller and cheaper satellites.

ASAT Readiness

Unless steps to increase the readiness of ASAT weapons could be kept secret in a crisis, such preparations would likely be destabilizing, even if preparatory actions could be seen as prudent from a technical perspective. A destabilizing finding, for example, may suggest that China is readying its ASAT-equipped SC-19 or that the United States is preparing SM-3 interceptors for space control missions. A related concern is that the United States may not have high confidence in its ability to detect or correctly interpret preparations for ASAT use. Covertly deployed ASAT capabilities that were suddenly made known could reduce incentives by the other side to attack, though the revelation would likely heighten tensions.

ASAT Exercises/Tests

A test of an ASAT weapon or a system that credibly could serve as an ASAT weapon generally would be destabilizing in a crisis, though such a test could add clarity to the crisis if explicitly intended and communicated as a signal. While such signaling is valuable, a test would nonetheless be potentially destabilizing and almost certain to provoke some adversary counter-response. Moreover, a failed test—a distinct Murphy's Law possibility—could actually weaken the potential attacker's credibility.

Rendezvous and Proximity Operations

Rendezvous and proximity operations will increasingly become a feature of future space operations. Certain kinds of on-orbit operations, such as repairs and replenishment of consumable resources, could enhance space deterrence and crisis stability by making satellites at least somewhat more resilient. Other kinds of on-orbit operations, including activities conducted in the vicinity of adversary space assets, would appear threatening to the adversary and would likely be destabilizing. Developing "rules of the road" for space operations would help to reduce, though not eliminate, potential instability from such operations. Keep-out zones around satellites, advance notifications, and other potential steps also deserve to be discussed and considered by governments for military, diplomatic, and economic reasons.

Dialogue

The single most important potential non-military action in any crisis is to initiate or intensify dialogue with the adversary. The effectiveness of dialogue will be greatly aided if related discussions have already taken place, enabling players to become familiar with each other and the issues involved. This is one of the arguments for major space powers to pursue discussions of a space code of conduct or rules of the road. U.S. efforts to initiate such discussions with China have been unsuccessful to date, but there is reason to believe this Chinese reluctance is not permanent, based on private Track 1.5/Track 2 discussions in which this author has participated.

Signaling

Signaling in a crisis is important, and it is more useful if accompanied by a "diplomatic libretto" to ensure that the intended message of an action taken, or not taken, is what is heard by an adversary. This is one more argument supporting space code of conduct/rules of the road discussions and strategic space dialogues among major space powers: in the absence of a clear understanding of what different space signals might mean, such signals are at serious risk of being misinterpreted by decision-makers who, in a crisis, will likely be mistrustful of one another and inclined to engage

in worst-case thinking. Likewise, unintentional or false signals, potentially caused by benign equipment failures, also can be destabilizing in a crisis, as participants scrutinize every significant event for its meaning and intent. One urgent task for space-faring countries should be to establish a libretto for space signaling, as well as a "choreography" for the transmission of such signals. North Korea's late-2012 space launch ironically illustrated the value of common practices in this arena; while the test clearly violated United Nations Security Council resolutions, North Korea slightly eased Western anxieties by providing advance notice of the launch and its purported intent, and by announcing a flight path that later matched the trajectory of the actual rocket. Still, there is justified concern that this "space launch" was in fact a step to develop an intercontinental ballistic missile (ICBM) using identical or similar technology. In short, the launch was an improper step conducted properly, in a manner that served North Korea's perceived security interests. The issue of signaling is further discussed on page 95[c], in the section authored by Blair and MacDonald.

Nuclear Force-Supporting Infrastructure

Actions that indicate any interest in targeting the key space infrastructures that support nuclear forces would be extremely destabilizing, as they would suggest (accurately or inaccurately) that preparation is underway for potential nuclear conflict. Likewise, cyber actions targeting the supporting infrastructure of nuclear forces would be highly destabilizing. Certain non-state actors may be attracted to such actions precisely for their destabilizing nature, and decision-making and planning must reflect this possibility.

States also must account for considerable differences between the nuclear force-supporting space assets of each space power. For example, the United States places high value on its missile warning satellites (SBIRS and DSP), which as yet have no Chinese analogue. Each launch-detection system provides essential support to U.S. ballistic missile defenses, which concern China for their feared potential to weaken or undermine Chinese strategic nuclear deterrence and enable greater U.S. belligerence toward Chinese interests.[83] As a result, China may have high incentive to attack DSP and SBIRS as a crisis transitions into conflict. In that way, "once early warning capability has been neutralized, attacks can be carried out on other components of the system, such as radar and missile systems."[84]

Further complicating space crisis stability is the unavailability of any assured second strike-like space capability for the short- to medium-term future. Several conditions

exist for promoting potential and actual stability in lieu of such a capability, though they are not equally available to major space players:

- Risk aversion that grows rapidly with escalatory actions
- Unknown collateral effects from space asset attacks, including effects that accelerate with escalation and time
- Rapid globalized interconnection that favors alliances and may inhibit Chinese actions
- Prospect of greater space resilience[d] of U.S. and other space architectures
- An ability to offset space deterrence limitations with capabilities from other domains

Considered in isolation, certain relatively modest offensive-oriented and offensive space actions would not be highly likely to lead to escalation in space. The history of warfare includes many precedents for electronic tactics such as radar jamming, and short of a major regional assault on a large number of satellites, limited jamming would not necessarily lead to escalation unless its combat role proved to be decisive. Strategically, space stability is likely to be fairly tolerant of lower-level offense, highly intolerant of major strategic-level offense, and of highly uncertain tolerance toward intermediate levels of offense, adding another element of ambiguity that national leaders will need to address in a crisis.

Space Stability

The importance of space stability has been recognized for some time, as in the 2009 final report of the Congressional Commission on the Strategic Posture of the United States (chaired by former Defense secretaries William Perry and James Schlesinger), which urges the United States to "develop and pursue options for advancing U.S. interests in stability in outer space."[85] The 2010 U.S. Space Policy also "recognizes the need for stability in the space environment."[86]

SEIS lie at the heart of U.S. military superiority and are an essential force multiplier, but the strategic importance of space is a two-edged sword for the United States and any other space-dependent country. Until space technology changes, space largely will be an offense-dominant environment, as then-Vice-Chairman of the Joint Chiefs of Staff General James Cartwright and others have pointed out. Thus, assets that greatly enhance our military power are also quite vulnerable, at least to space near-peers.

The strategic implications of this situation are troubling, and they are made more so by the advancing technology of the space and cyber domains.

While nuclear weapons are certainly terrifying in the abstract, they are less destabilizing than offensive counter-space capabilities due to their immense destructive potential, the high likelihood that their use would prompt escalation in a conflict, and confidence that a nuclear retaliatory capability would survive a first strike. Space weapons are more potentially highly destabilizing in a crisis due to their more focused destructive nature, their greater likelihood of use, their potential to significantly damage conventional and possibly nuclear C4ISR capabilities from space, and the advantages they could provide to whichever party strikes first. Offensive counter-space weapons appear much likelier than nuclear weapons to be used in the early transition from a crisis to an open conventional conflict between the United States and a major power such as China. Space includes no assured second-strike capability analogous to the Fleet Ballistic Missile Submarines (SSBNs) and submarine-launched ballistic missiles (SLBMs) of the nuclear domain, as noted earlier. The United States could ameliorate this worrisome state of affairs by rendering vital SEIS sufficiently resilient to attack (through disaggregation, fragmentation, or active defense) that the services could continue to adequately function after absorbing a major first strike. Such a condition appears unlikely in the near- to mid-term, however.

As noted earlier, an inherent risk of strategic instability exists when relatively modest defense efforts create disproportionate danger to an adversary, as with space offense. A serious risk of crisis instability exists in space when a space power would benefit from acting first in a crisis to destroy an adversary's satellites, rather than risk the destruction of its own satellites in an adversary first strike. Indeed, high strategic payoff from pre-emption virtually defines the term "crisis instability." It is unclear what would happen in a crisis, but the potential for space instability seems high and likely to grow.

A risk-averse U.S. space strategy generally would aim to keep the space domain free of offensive action for as long as the United States derived greater military and other benefits than other countries from space and SEIS. While offensive space action could benefit the United States in some instances, such action could place at risk the military advantages it currently enjoys in space, given the domain's largely offense-dominant nature. A U.S. decision to employ space offense in a crisis or conflict must weigh this trade-off carefully.

Most major offensive actions against adversary space assets would represent a step into a conflict realm in which no country has much, if any, experience. The unintended consequences, which may include major disruptions arising from unforeseen infrastructure interdependencies, would probably pose some disincentive—though not an absolute barrier—to major offensive actions.

It is possible in any crisis for conflict to become inevitable, despite the intentions of the parties involved. In this context, another key objective for the United States and any adversary country would be to avoid sparking conflict through miscalculation or misunderstanding, as happened commonly in the twentieth century. The central challenge for major space powers is to build firebreaks of sufficient resilience and effectiveness that unstable escalation can be avoided, so any escalation in space is at least based on an accurate understanding of the developing space situation. Such firebreaks, to the extent that they can be implemented, are important for addressing both planned as well as unplanned or inadvertent conflict.

Strategic offensive space operations in peacetime are highly unlikely in much the same manner that a "bolt-out-of-the-blue" nuclear attack was unlikely during the Cold War, though the latter scenario was a force planning consideration in that era. In general terms, it would be prudent to assume that any apparent offensive action of little more than nuisance impact is a one-off occurrence: possibly an accident or a rogue event, or at most a way to demonstrate capabilities and send a signal. A prudent response would include a modest increase in defensive alert level, probably accompanied by a priority request for explanation from an appropriate level of the suspected country of origin. Related communication would be most easily accomplished through a modality comparable to the U.S.-Russian Risk Reduction Center, or "hot-line," assuming such a mechanism had been instituted with the relevant country to address space issues. The United States, then, should consider expanding the coverage and capabilities of the U.S.-Russian "hot-line" and creating new space hotlines with other space-faring nations. It bears mentioning, however, that information exchanged through such channels would be subject to extra scrutiny by both sides for fear of potential deception, a valid concern.

FEATURES OF CRISIS STABILITY IN SPACE IN THE YEARS AHEAD

Future Technologies and Their Crisis Stability Implications

It is likely that future technologies will profoundly affect the space domain not only through their information and other services, but also through their offense and defense capabilities. ASAT and BMD capabilities share some common characteristics and dynamics. In general, both have limitations, but disruptive new technologies may overturn many assumptions about their respective possibilities and dynamics. Specifically, current BMD concepts rely on expensive kinetic interceptors that cannot realistically be procured in large numbers, much less their supporting radars and command-and-control systems. Major advances in directed-energy weapons, such as high-powered lasers, could radically reduce the cost-per-shot if the technology can ever be mastered. While such developments have not happened yet at any significant scale, they cannot be dismissed out of hand, given the stakes involved. Accordingly, discussions of more resilient and survivable space architectures should be accompanied by discussion of the potential for new BMD and ASAT technologies.

The United States has made no secret of its objective to develop more resilient space architectures. Technologies to enable highly disaggregated U.S. architectures would represent at least a temporary revolution in space, presenting China or any other putative adversary with a more numerous and highly diffuse set of targets, greatly complicating its offensive requirements. Furthermore, resilience is unlikely to be a one-size-fits-all phenomenon. The technical tasks of some space-based assets may be easier than others to disperse across a larger number of components. Resilience also may be further enhanced relatively inexpensively through "decoy disaggregated components" that simulate the external behavior of actual components.

One important non-technical obstacle to radically new space technologies, including a highly disaggregated architecture, is a broad institutional preference for legacy space architectures that involve highly complex individual satellites with which professionals are more familiar and therefore feel more comfortable developing and using. Disaggregation is not universally accepted as an important means to achieve such space

resilience, though it is one of several options of intense interest to the U.S. Air Force. (Arguments for disaggregation apply to both space- and ground-based elements of the space architecture.)

If the United States were somehow able to provide a level of assured functionality to the space- and ground-based assets that enable connection with the force-multiplying SEIS stream, the benefits for space crisis stability would be immense. A major first-strike attack would not prevent U.S. space assets from functioning with sufficient effectiveness to provide crucial military and intelligence information to U.S. decision-makers and military forces. The "Space" column of the page 44 table would look substantially different. At a minimum, any resilient space asset architecture must embody a significant degree of excess capacity, given that a major first strike would likely destroy at least some capability. Attaining such a capability for the offense-dominant environment of space will require new technological and architectural concepts.

At least three broad technology thrusts, which are not mutually exclusive, hold promise to achieve such a level of functioning resilience, at least in combination. In order of increasing conceptual complexity, the first would be an operationally responsive space (ORS) posture that provides substitute capabilities for a limited time after an adversary first strike before they too are neutralized by adversary force. If an ORS posture could buy enough time for U.S. forces to achieve their objectives prior to the destruction of backup satellites, such a posture could discourage escalation in space. However, it would be difficult to maintain a robust ORS posture in the face of constant technological adaptation by adversaries. In addition, if ORS assets were rapidly deployed prior to an outbreak of hostilities, the step would likely be perceived as preparation for conflict and therefore be destabilizing. (Once conflict began, an ORS posture's destabilizing potential would cease to be a major concern.) Another drawback to ORS is its potential cost, especially for the short-term replacement of sophisticated satellites for intelligence gathering and other functions. Besides cost, such satellites would be vulnerable once in orbit, unless offensive action in other domains negated adversary offensive capabilities. Future ORS feasibility may increase to the extent that small satellite technology and miniaturization more generally reduce satellite cost. One technology initiative of the U.S. Defense Advanced Research Projects Agency (DARPA), the Airborne Launch Assist Space Access (ALASA) program, may improve ORS feasibility by enabling a fairly small, aircraft-fired rocket to deploy small, 100-pound satellites in a manner that is relatively inexpensive (less than $1 million) and prompt (within 24 hours).[87]

The second technology thrust would rely on a *proliferated, disaggregated architecture for space assets*. This approach, which is quantitatively and qualitatively different from ORS, would distribute the capabilities of a smaller fleet of complex satellites over a much larger number of smaller, specialized satellites capable of interacting with one another to recreate the capabilities of the larger satellites, while presenting many more targets for an adversary. In theory, this architecture would greatly complicate any effort to disable U.S. space assets and deny SEIS benefits, in a manner similar to the use of multiple warheads both as a countermeasure to ballistic missile defense and as a means to increase ballistic missile effectiveness. Such an approach would seem to embody the resilience that has been identified as a major design objective of future U.S. space architectures.

This proposed architecture is not unlike the survival strategy in nature of some cicadas, which have evolved a brute force strategy of reproducing in large numbers to ensure that a small but sufficient percentage survives to perpetuate the species, despite major attrition in initial numbers. This defense against predation is known in biology as predator satiation: because so many emerge at once, the number of cicadas in any given area exceeds the number that predators can consume; all available predators are thus satiated, and the remaining cicadas can breed in peace.[88] Although crude, this strategy appears to have allowed cicadas to survive and prosper for millennia and more. In like manner, a "cicada strategy" of deploying far more disaggregated satellites than a space offensive capability can attack could in theory achieve mission resilience, though it would involve an uncertain cost trade-off. Space assets have a major advantage that cicadas do not: the "predation" numbers are nowhere near as daunting, and offense in other strategic domains can further reduce the number of "predators." If a sufficiently large number of disaggregated satellites can be orbited, a "predator country" may be dissuaded from attacking in the first place, as it would likely fail in an attempt to seriously compromise U.S. space capabilities.

The third technology thrust would be a high-altitude aeronautical alternative backup comprised of assets that would not be vulnerable to counter-space weapons because they would, in effect, be shielded by the atmosphere. This approach also may help buy enough time to allow U.S. forces to be effective, though there still would be no guarantees, and China or another advanced adversary would actively seek ways to counter such a capability. This option apparently is being explored by the U.S. Missile Defense Agency, according to published reports.[89] The approach also has been explicitly cited in the "Third Offset" report of the Center for Strategic and Budgetary Assessments, which some observers have asserted reflects the thinking of Robert

Work, the current deputy secretary of defense as of 2016. It notes that "space is no longer a sanctuary from attack."[90] It later describes the potential capability:

> "In peacetime, this capacity would complement space-based remote sensing, which can provide near-global coverage… Unmanned aircraft could provide a surveillance "stare" capability that cannot currently be provided by satellites. From international airspace, they could peer into the territory of prospective adversaries. In wartime, unmanned aircraft would provide a critical operational hedge against the loss of space both for ISR, precision navigation and timing [i.e., GPS… and long-haul communications. An expanded, air refuel-able unmanned aircraft fleet could provide a responsive, geographically distributed, sustainable, scalable surveillance-strike capability."[91]

This approach embodies the essence of resilience. Rather than actively defending space assets, a more difficult task, it hedges against adversary offensive counter-space capabilities by rendering them less effective and thus less valuable as targets to an adversary. It would not only provide continuing capability (though enemy offense may cause some degradation of peacetime capability), but it could also discourage China or any other adversary from aggressively seeking offensive counter-space capabilities in the first place, as they would be far less effective than against a much smaller number of highly sophisticated satellites. As China's economic growth slows to a more subdued level,[92] Beijing will face more difficult military budgetary decisions that such a U.S. capability could influence.

Other more exotic technologies may become available further in the future. Ground-based high-energy lasers with adaptive optics could actively defend satellites against approaching threats, as well as attack satellites directly. Meta-material-based cloaking technologies under investigation by DARPA[93] could also hinder adversary offensive space assets in a conflict.

While some combination of these and other approaches may result in resilient U.S. space capabilities, it is unclear when the United States may achieve space resilience and how long it would last. Precisely because U.S. space capabilities are a significant force multiplier, China or other potential adversaries would likely strive to develop countermeasures to such resilience. The success of any adversary countermeasures is impossible to predict, but they would almost certainly be pursued. Meanwhile, the United States would seek to preserve its space resilience, and it would likely pursue

means to overcome future adversary space resilience to meet the space control requirements of U.S. space policy.

Thus a central issue for the years ahead is the extent to which space can be a resilient domain. At present, the space domain has no equivalent to the nuclear domain's sea-based nuclear forces, which are able to withstand a full nuclear attack and respond with a devastating counterattack. Indeed, the single most stabilizing aspect of the strategic nuclear balance remains the SSBN/SLBM element, whose high survivability is an important stabilizing component of the strategic nuclear balance. It is no coincidence that Russia is today modernizing its sea-based deterrent, in part by deploying an SLBM that is very roughly comparable to the Trident II that the United States began to deploy in 1989. China and India are introducing credible ballistic missile submarines into their nuclear arsenals, and the United States has begun to develop a new SSBN and accompanying missile. Each of these projects recognizes the assured survivability and deterrent value of a submarine-based nuclear deterrent. The apparent absence of such a stabilizing element in the space and cyberspace domains is a major obstacle in achieving space and cyber stability. Whatever "assured retaliation" space asset a country may deploy, it would likely contribute to a future space equivalent of the Cold War-era submarine-antisubmarine competition.

The absence of a compelling assured second-strike space capability comparable to the submarine-based missiles of the nuclear domain, coupled with the increasing vulnerability of space assets in the near term, paint a bleak picture of space crisis stability, at least until the U.S. space posture becomes much more resilient in the face of potential attack. In the interim, at least two factors mitigate this apparent instability: (1) deterrence from other domains where the U.S. ability to retaliate decisively is still intact; and (2) the lack of full confidence that China, or any other potential U.S. adversary, could have in the success of a first strike in space. Neither of these factors is anywhere near as robust a deterrent as submarine-based missiles are in the nuclear domain, but their effect is not negligible at strategic levels of decision-making and cannot be ignored.

One problem of such cross-domain deterrence as a substitute for space resilience is the issue of credibility. The United States is unlikely to execute a nuclear retaliation against a major and successful Chinese attack on U.S. space infrastructure that does not directly support U.S. nuclear forces, and even an attack against U.S. nuclear command-and-control elements would not necessarily provoke a U.S. nuclear response. A major U.S. conventional response would be more likely, but the inciting attack

may have seriously hampered capabilities for such a response by cutting off U.S. conventional forces from SEIS. Moreover, the inevitable loss of life on both sides would inflame passions for revenge within both countries, an important escalation enhancer that renders any major conventional conflict a far-from-ideal scenario. More likely still would be a major U.S. retaliation in cyberspace against China, though here the problem would be uncertainty over both the attacks' technical effectiveness and the difficulty of assessing damage to an adversary. Likewise, in the crisis phase preceding such an attack, Chinese decision-makers would face similar uncertainty about the effectiveness of an anticipated U.S. retaliation in cyberspace. These observations introduce the key role of uncertainty in the space and cyber domains, which exceeds even its role in the conventional and nuclear domains.

It is also important to remember the threat from Murphy's Law, which colloquially states: "anything that can possibly go wrong, will." No government is ideally established to deal with crises, and some are less prepared than others. Tactics often overwhelm strategy in a crisis, and senior leaders often participate in decisions for which they are unprepared. These institutional shortcomings were less dangerous even with regard to nuclear weapons, for which capabilities, strategies, and tactics became relatively well understood over the decades. Now with two major new and highly technical domains, space and cyber, thrust into prominent military roles, understanding among senior leaders has probably reached historic lows. Yet surrendering such decisions to an "expert class" is anathema to political leaders when so much is at stake, and not without reason: technical experts are often unqualified to make major political calls far beyond their specialized expertise.

Furthermore, history holds many cautionary tales about the influence of random events on military decisions and outcomes. An unexpected coup in Yugoslavia delayed Hitler's 1941 attack against Russia by a crucial, and fateful, month; had Nazi Germany attacked that May rather than in June, Hitler may have had time to capture Moscow before the following brutal winter.[94] In 1962, China shot down a U-2 reconnaissance aircraft and prompted the United States to curtail U-2 flights, likely delaying discovery of the Soviet missile emplacements in Cuba that became the focus of the Cuban Missile Crisis. In 1973, U.S. Vice President Spiro Agnew's resignation and the notorious "Saturday Night Massacre" coincided with Egypt's attack on Israel, resulting in Secretary of State Henry Kissinger—not President Richard Nixon—deciding most U.S. actions in the latter crisis. Uncertainty and random events are endemic to crises, yet the stakes in crises are high and quick decisions are necessary, even amid uncertainty and unpredictability.

After decades in which the vulnerability of space assets raised relatively little anxiety, the growing concerns of the last ten years have sparked serious consideration of technical, policy, and diplomatic approaches to these problems. Though details on technological options are scarce and no "silver bullet" solution is yet visible, several approaches appear to offer important possible means to improve the resilience of overall U.S. space capabilities. The next section explores other features of the strategic space landscape that may offer some cause for hope.

Uncertainty and Hysteresis in Space and Cyber Deterrence

What is to be done in lieu of technological solutions that are not yet available? Is space in fact highly unstable at present, and will it be so going forward?

Resilient and redundant space assets will be key to deterrence and crisis stability in space. While only minimal efforts will likely be sufficient to address relatively unsophisticated space and cyber threats, the United States will require system resilience, alternative backup systems, and other means to preserve core SEIS capabilities in the event of conflict with a major space-faring nation. Resilience and redundancy will enhance crisis stability to the extent that the United States can successfully embed these features in its space systems. As China seeks to extend its military reach farther from its territory, the PLA will rely more on space to meet its growing requirements for global and space situational awareness. This growing space dependence will complicate PLA contingency planning, as greater reliance on space almost certainly will be accompanied by greater space vulnerability. The PLA will also likely seek more resilient and redundant space capabilities, and it is rightly "concerned about… protecting China's growing interests in space."[95]

In any crisis that threatens to escalate into major power conflict, political and military leaders will face uncertainty about the effectiveness of their plans and decisions. This uncertainty will be compounded when potential conflict extends to the space and cyber domains, where weapon effectiveness is largely untested and uncertain, infrastructure interdependencies are unclear, and damaging an adversary could also harm oneself or one's allies. Unless the stakes become very high, no country will likely want to gamble its well-being in a "single cosmic throw of the dice," in Harold Brown's memorable phrase.[96]

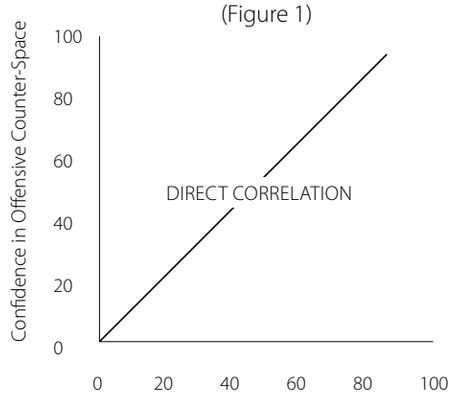
The novelty of space and cyber warfare, coupled with risk aversion and worst-case assessments, could lead space adversaries into a situation of what can be called "hysteresis," where each adversary is restrained by its own uncertainty of success. This is

conceptually shown in Figures 1 and 2 for offensive counter-space capabilities, though it applies more generally.[97] These graphs portray the hypothetical differences between perceived and actual performance capabilities of offensive counter-space weapons, on a scale from zero to one hundred percent effectiveness. Where uncertainty and risk aversion are absent for two adversaries, no difference would exist between the likely performance of their offensive counter-space assets and their confidence in the performance of those weapons: a simple, straight-line correlation would exist, as in Figure 1.

The more interesting, and more realistic, case is notionally presented in Figure 2, which assumes for simplicity that the offensive capabilities of each adversary are comparable. In stark contrast to the case of Figure 1, uncertainty and risk aversion are present and become important factors. Given the high stakes involved in a possible large-scale attack against adversary space assets, a cautious adversary is more likely to be conservative in estimating the effectiveness of its offensive capabilities, while more generously assessing the capabilities of its adversary. Thus, if both side's weapons were 50% effective and each side had a similar level of risk aversion, each may conservatively assess its own capabilities to be 30% effective and its adversary's weapons to be 70% effective. Likewise, if each side's weapons were 25% effective in reality, each would estimate its own capabilities to be less than 25% effective and its adversary's to be more than 25% effective, and so on. In Figure 2, this difference appears, in oversimplified fashion, as a gap that represents the realistic worry that a country's own weapons will under-perform while its adversary's weapons will over-perform in terms of effectiveness. If both countries face comparable uncertainty and exhibit comparable risk aversion, each may be deterred from initiating an attack by its unwillingness to accept the necessary risks. This gap could represent an "island of stability," as shown in Figure 2. In essence, given the enormous stakes involved in a major strike against the adversary's space assets, a potential attacker will likely demonstrate some risk aversion, possessing less confidence in an attack's effectiveness. It is uncertain how robust this hysteresis may prove to be, but the phenomenon may provide at least some stabilizing influence in a crisis.

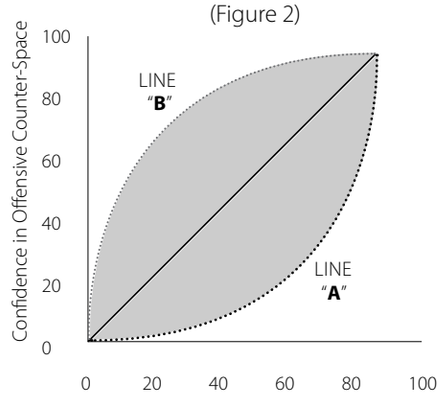
No Hysteresis Island of Stability

(Figure 1)



Hysteresis Island of Stability

(Figure 2)



In the nuclear domain, the immediate, direct consequences of military use, including blast, fire, and direct radiation effects, were appreciated at the outset. Nonetheless, significant uncertainty and under-appreciation persisted with regard to the collateral, indirect, and climatological effects of using such weapons on a large scale. In contrast, the immediate, direct effects of major space conflict are not well understood, and potential indirect and interdependent effects are even less understood. Indirect effects of large-scale space and cyber warfare would be virtually impossible to confidently calculate, as the infrastructures such warfare would affect are constantly changing in design and technology. Added to this is a likely anxiety that if an attack were less successful than planned, a highly aggrieved and powerful adversary could retaliate in unanticipated ways, possibly with highly destructive consequences.

As a result, two adversaries facing potential conflict may lack confidence both in the potential effectiveness of their own attacks and in the ineffectiveness of any subsequent retaliation. Such mutual uncertainty would ultimately be stabilizing, though probably not particularly robust. This is reflected in Figure 2, where each side shows more caution than the technical effectiveness of its systems may suggest. Each curve notionally represents one state's confidence in its offensive counter-space effectiveness relative to their actual effectiveness. Until true space asset resilience becomes a trusted feature of space architectures, deterrence by risk aversion, and cross-domain deterrence, may be the only means for deterrence to function in space.

During the Cold War, the numbers and kinds of nuclear weapons in the U.S. and Soviet arsenals were well known and widely published in the United States. The large and observable nature of these weapons, coupled with U.S. declassification of much of this information, allowed a level of peacetime transparency and understanding that is not characteristic of the space and especially the cyber domains today. The present lack of space and cyber transparency adds to uncertainty on both sides, though it is safe to assume there is greater knowledge of space and cyber forces at the classified level, well beyond the purview of this report. This greater knowledge, however, is unlikely to be as extensive as knowledge of nuclear forces. In crisis and conflict planning, the United States and others would likely hedge their bets and assume relative worst-case space and cyber force postures for their adversaries. The probable uncertainty from such worst-case planning would be self-deterring to an unknown extent: countries in crisis would fear a particularly effective retaliation to a potential attack, and would therefore be less inclined to breach the threshold of conflict. This uncertainty factor is likely a stronger planning influence for cyber conflict than space conflict, but it probably most affects nuclear weapons, given their huge destructive capabilities. Uncertainty would also vary with abilities to attribute space, cyber, or other attacks to any specific country; a potential attacker may be encouraged to carry out a strike to whatever extent it believed it may not be linked to the attack. Attribution abilities for attacks on space assets are thus critical to crisis stability in space. In general, risk aversion or hysteresis effects will likely increase with the size of the initial attack under consideration.

To a limited extent, then, this hysteresis in the space and cyber domains is a weak analogue to the SSBN/SLBM leg of the nuclear triad, which threatens a devastating response to a first strike. That is, a country contemplating a first strike or escalation must weigh the possibility that its adversary has substantially greater space and/or cyber capabilities than perceived, and a potential initial strike thus may be less effective and prompt greater retaliation than expected. In this case, however, the assurance and extent of a devastating response are less certain than for sea-based nuclear weapons, and thus the deterrent effect is less assured. However, in the search for crisis stability, we must take our silver linings where we can find them.

An interesting question is whether deterrence is helped or hurt by greater transparency of space capabilities, offensive or defensive. While transparency is generally desirable for a more stable space environment, its value becomes more difficult to assess in this case, where uncertainty strengthens the risk aversion that would be a relatively stabilizing influence in a crisis. Yet deterrence requires an adversary to have at least some reason to believe that its opposition possesses more than a trivial offensive capability. There is no clear answer here, but a case can be made for a "Goldilocks approach": not enough transparency to provide a militarily inferior adversary with serious incentive to strike first rather than second, but still enough to concern that adversary with one's own offensive space capability.

The U.S. public, and most lawmakers and the executive branch officials, have no sense of their country's offensive space capability; ironically, they receive more information about the qualitative nature of China's capability. Questions about U.S. offensive space capability, including broad inquiries about the feasibility of space deterrence in the absence of such capability, are routinely turned aside when submitted to administration officials. A clear tension between opacity and transparency persists on this matter, and the executive branch appears to have opted for opacity, for which a good case can be made. Even if this opacity is preserved, the trade-off would benefit from more inclusive public discussion. This issue remains largely unaddressed to date, but it will be more difficult to ignore as military considerations in space continue to increase over time.

The Role of Resilience in Space Security and Crisis Stability

The central challenge in designing and building a stable and robust space architecture is to enable that architecture to withstand a major adversary attack and remain capable of meeting its mission requirements. In the nuclear domain, as discussed earlier, all three legs of the nuclear triad have considerable levels of survivability against a first strike, but the SSBN/SLBM combination is probably the premier asset in this regard. This element of survivability is missing from space at present, which illustrates why resilience is seen as an important objective, and a "key criterion in evaluating alternative architectures."[98]

Resilience is rightly seen as an important aspect of crisis stability, and while it is a frequent subject in discussions of space architectures, it is generally not discussed in public with any depth. If achieved, a resilient space architecture would largely blunt or negate the effectiveness of an adversary's offensive space capabilities, greatly reducing their deterrent value while enhancing the deterrent effect of the overall forces of that architecture. General John Hyten, commander of U.S. Air Force Space Command, succinctly stated the importance of space resilience to his service and to U.S. security interests more generally: "I guess because we're space people and we're geeks and we put numbers on everything, but I don't care what the [resilience metric] number is. I want a resilient war-fighting construct."[99]

The Air Force defines resilience as "the ability of a system architecture to continue providing required capabilities in the face of system failures, environmental challenges, or adversary actions."[100] In a similar vein, the Department of Defense fact sheet on the resilience of space capabilities states that "the purpose of resilience is to assure performance of military and related intelligence functions at a level necessary to execute assigned missions within an acceptable tolerance for risk."[101]

According to the fact sheet, the new space asset "focus is on 'disaggregating' space capabilities onto multiple platforms or systems. Disaggregation improves mission survivability by increasing the number and diversity of potential targets, thereby complicating an adversary's decision calculus and increasing the uncertainty of successful attack."[102] Once again, enhancing adversary uncertainty assumes a key role in space architecture design. In addition, such disaggregation would make U.S. space capabilities more resilient against completely benign challenges, such as orbital debris, solar flares, and unexpected satellite malfunctions. Operational concepts for disaggregation are necessary to flesh out its promise, as a 2014 Government Accountability Office report has noted.[103]

This approach includes one ironic dimension: by reducing the damage that the loss of a single satellite would cause to an overall space system, disaggregation would make an attack on one satellite less provocative than if such a strike resulted in major system degradation. At the margin, then, disaggregation would reduce disincentives to escalate in space while also greatly reducing the effectiveness of a space attack, with the latter impact likely outweighing the former in a properly designed architecture.

This emphasis on resilience plays a comparably large role in planning in the cyber domain, where lower-level "conflict" is an ongoing fact of life. There, too, resilience is a key objective for planners. As the top cyber-security official at the Department of Homeland Security, Phyllis Schneck, puts it, "our job is to make sure that the resilience is here" in critical infrastructure networks, both within the federal government and in the private sector, to ensure that networks can operate even when under attack.[104]

Despite the appeal of this vision of effective space and cyber resilience, a number of caveats are in order. At a minimum, resilience is probably a relative term, dependent on variables such as scenario, time, and conflict duration. As a result, a crying need exists for metrics to evaluate resilience (despite the likely difficulty of measuring this attribute) and to ensure that different approaches can be measured and evaluated on an apples-to-apples basis. The Government Accountability Office report notes this need for resilience metrics, observing that the Department of Defense "does not have common measures for resilience—a key space system consideration."[105] Resilient disaggregated architectures probably present operation and integration challenges, as a flotilla of disaggregated small satellites would be more challenging to manage and control than one large, though more vulnerable, satellite.

According to the Department of Defense, "the primary measure of resilience at the Enterprise, Mission, and Functional levels is risk to national security objectives, mission effectiveness, or functional capability,"[106] but this definition includes no additional context. In addition to risk, the severity and duration of any shortfall in capability after an attack are key criteria in assessing resilience. Another issue is more technical: can key space asset capabilities be disaggregated to a point that sufficient survivability is assured? Complex intelligence satellites may pose a greater disaggregation challenge than communications satellites, though the survivability payoff in either case would be substantial.

One important option is to disaggregate not only by satellite function but also by operating altitude. Integrating "atmospheric satellites" into a space architecture would pose an entirely new challenge to an adversary's offense. Such a mixed system could have important benefits, given the different vulnerabilities, operating altitudes, and environments of its components. In view of the higher operating costs of aeronautical systems, they could be operated on an occasional peacetime basis and pressed into more active service in a crisis, adding another dimension to resilience and sending a signal of resolve to friend and foe alike.

Another caution on resilience comes from decades, even centuries, of human military experience: nations do not remain passive in the face of important adversary military developments. They react with countermeasures to try to offset their adversary's advantage, and often attempt to replicate for themselves the new adversary capabilities. This historical lesson emphasizes the importance of examining potential resilience countermeasures. What kind of countermeasures might the United States expect, even if it achieves a (perhaps temporarily) resilient space architecture? An offensive capability characterized by a low marginal cost per shot, such as lasers, is one possible approach. Another countermeasure might incorporate tactical electromagnetic pulse (EMP) effects, which potentially could target a disaggregated space architecture by hitting satellites at particular times and places (depending on the spatial separation of the satellites) rather than destroying all of its components. Tactical

EMP and cyber attacks against ground stations are other countermeasures, and other options are likely as well.

These cautions are not intended to challenge the value of pursuing space resilience. The United States certainly should pursue resilience in a reasonable and deliberate fashion, but with eyes wide open to the likelihood that the advantage of any given approach may well be more fleeting than final. Any particular approach probably will not be enduringly resilient; its resilience will likely degrade over time, requiring new resilience measures to compensate. Adversaries will develop countermeasures that the United States will need to address with counter-countermeasures, and so forth. In short, the age-old race for military superiority will extend to the reaches of near-space. In any case, space resilience will be not just a desirable goal, but also a key element in reducing crisis instability and boosting U.S. deterrence capabilities.

The United States must consider at least two additional factors in pursuing space architecture resilience:

- How will the United States address adversary resilience?
- Would resilience create "moral hazard" concerns?

It would be a mistake to believe that China and perhaps others would not try to achieve some comparable resilience for their space assets. If the United States has any interest in potentially negating another country's space assets, then a dynamic measure-countermeasure competition will be inevitable and possibly costly, given the importance of space and the stakes involved. Such a resilience competition would likely have mixed implications for crisis stability, depending on the effectiveness of the countermeasures it entailed. On balance, however, such competition would probably increase uncertainty in the strategic calculations of major powers, thereby inducing greater risk aversion in a manner that would be stabilizing, though perhaps not particularly robust.

Another space resilience issue is that of moral hazard: possessing a level of protection against an adversity enables greater risks of the type that the protection was intended to prevent. For example, a person may buy car insurance and then drive more recklessly. Would space resilience, to the extent it is achieved for any period of time, allow a country to take bolder risks in space than it otherwise might during a crisis? The answer is not clear, but some effect of this nature appears entirely possible. Moral hazard questions further add to the unknowns that characterize the space domain, making crisis decision-making even more difficult and uncertain.

In arguing for a new global surveillance and strike concept, the Center for Strategic and Budgetary Assessments envisioned a key role for resilience and specifically identified space systems as a major opportunity. Such a concept would be "Resilient in that it would be geographically distributed with minimal dependence upon close-in bases, have a greatly reduced sensitivity to enemy air defense capabilities, and be significantly more tolerant of disruptions of space-based systems [emphasis in the original]."[107]

The more general advent of commercial satellite imagery and smaller satellites—including "small-sats," "micro-sats," and "nano-sats"—are narrowing the capability gap between the United States and its adversaries and leading to what some observers have dubbed the "democratization of space." Emerging space capabilities would be available not just to peer space powers but also to countries of far lesser space capabilities. Such democratized space capabilities probably will not be resilient, but they will add additional, evolving complications to the national security planning process in the United States and other countries.

To the extent that the United States achieves and sustains a resilient space architecture, it will realize an important benefit in addition to continued access to space during conflict: the assured functionality of U.S. space assets would reduce pressure on Washington to escalate a space conflict. This benefit could diminish, though probably not eliminate, U.S. requirements for space offensive capability if this resilience could somehow be maintained over time. This consideration shows again that space architecture resilience has a key role to play in promoting crisis stability in space.

SPACE DIPLOMACY AND SPACE SIGNALING

International and Other Options to Strengthen Crisis Stability

Victoria Samson

Space assets can both hinder and help crisis stability. They can be used accidentally or perhaps even intentionally to amplify poor relations between nations, possibly turning a tense situation into a crisis. Alternatively, they can clarify misunderstandings or false assumptions regarding the actions of a potential rival, thereby improving crisis stability.

A variety of options are available to strengthen space crisis stability, with an overall end goal of accounting for user intentions in employing various dual-use space technologies. Because intent can be either misconstrued or openly discussed, international approaches must strive to increase transparency about intent and policies. States can seek greater transparency in several multilateral fora and through international approaches that mostly derive their strength from shared norms of behavior for responsible space actors. Transparency also can benefit from technological approaches like space situational awareness data collection and dispersal. Furthermore, the decision-making calculus for crisis scenarios should incorporate domestic considerations for the United States and potential adversaries. Finally, certain actions can signal good intent and help to dispel misinterpretation of a space actor's behavior, which can then either minimize a crisis situation or prevent it from emerging at all.

International Fora for Stability and Space

International discussions strengthen crisis stability by building relationships, which are needed both for knowing whom to contact in times of emergency and also for understanding the context for decision-making in a crisis. Communicating intent—not adopting certain hardware—will be the primary means of signaling a nonthreatening posture in space, which raises questions concerning how to demonstrate responsible and non-hostile behavior on orbit. This issue is even more important when dealing with potential dual-use capabilities for active debris removal or rendezvous and proximity

operations; views of the intent behind any such program are intimately tied to views of the country in possession of the supporting technologies. It is occasionally easy to become absorbed in technical possibilities and to overlook the more vexing legal, policy, and political challenges of these programs, but space powers must address the latter issues in order to advance to the next stage in utilizing space.

Participating states should aim to improve information exchange through international discussions using several different methods. Such engagement can take place bilaterally through memorandums of understanding (MOUs), 2+2 talks (typically between the U.S. Departments of State and Defense and their counterparts in another country), trade agreements, and even military cooperation. Multilateral options include the United Nations, which has advantages (it is an established venue to which countries have already committed representation) and disadvantages (its pace of working is often slow and can be further hampered by unrelated contentious issues). While freer discussion is possible outside the UN system, other fora include added costs for attendance and their processes may require more time than allotted. Regional multilateral meetings, such as the Asia-Pacific Regional Space Agency Forum, are options for addressing space security and space stability, if the issues can be placed on their agendas.

International Approaches

Participants in international discussions have several options for seeking agreement among participants and, perhaps more importantly, demonstrating the consequences of not following through on agreements from the discussions. Their first option is to pursue norms of behavior, or non-legally binding approaches. Voluntary norms, or best practices, are regularly developed out of self-interest and are stronger when they are perceived as being legitimate—that is, when they appear both reasonable and credibly enforced. Because a norm must be accepted by most of the community it addresses in order to be considered representative of common practices, its initial negotiation often must strike a balance between inclusiveness and focus. In addition, talks must incorporate major actors in specific areas to ensure that the discussions cover the actual behavior of involved parties.

By describing standard behaviors, norms simplify efforts to identify behavior outside of what is regularly done. They establish shared understandings of behavior that is considered responsible, resulting in important standards to prevent possible escalation during times of crisis.

International treaties represent a wholly different approach: they depend on state negotiators, and they assume that individual participants have sufficient respect for the international system to abide by an agreement's legal mandates.

Norms and international treaties each have advantages and disadvantages. Norms of behavior support the development of relationships between key players; they build momentum for future cooperation and/or agreements; they allow discussions on difficult issues to commence without pressure to reach legally binding conclusions; and they encourage a bottom-up approach to international discussions. However, such agreements may address "low-hanging fruit" rather than more pressing international issues; they lack legal force; and understandings that do not represent the overall community may result in incomplete compliance.

Treaties have more legal force, as well as the additional credibility that comes from negotiation at a state level. However, their formulation requires broad participation; they may take longer to negotiate than norms of behavior; and concerns about burdensome legal obligations may prompt reluctance among potential signatory states.

International cooperation, or at least an international approach, to the complexities of space stability can help space stakeholders to clarify their intentions toward one another. Misperceptions or mistrust should not fill the gaps, as perceptions of space capabilities and behavior are strongly influenced by political realities on the ground. The establishment of norms of behavior, or a generalized agreement about what constitutes responsible use of space, may be of use in this regard. This goal can be accomplished via formal legal treaties, as well as through more informal, soft law approaches.

These international approaches to space stability are not mutually exclusive. In fact, they would together demonstrate a strong commitment to ensuring the long-term availability of space for pursuing national security and international stability goals. By participating in such efforts, each space power could express good intentions for its space program and limit any outside concerns about the goals of its space capability. These international efforts would contribute to a broader set of responsible behaviors that may lack legal force, but still would be considered relatively common practices that are responsibilities of all space-faring nations to carry out. Whether or not such international initiatives result in a perfectly stable space domain, the discussions would be helpful in and of themselves.

International Initiatives

There are four main treaties currently in force that provide the foundation for international space law. They are the 1967 Outer Space Treaty, which establishes principles governing the activities of states in the exploration and use of outer space, including the moon and other celestial bodies; the 1968 Rescue Agreement, in which the parties to the treaty agree to cooperate on rescuing astronauts who are in distress; the 1972 Liability Convention, which spells out liability of space activities and assets in space; and the 1974 Registration Convention, which requires the parties to register objects launched into space. In the decades since these treaties were negotiated, a preponderance of new actors and activities has created some gray areas that are not covered. As more countries increasingly depend on space for national and economic security, there is a growing recognition of the need to ensure that space is stable and reliable over the long term.

The degree to which crisis situations become destabilizing often depends upon the regional or international stability that existed prior to the crisis event. International space initiatives are key to establishing that baseline. The international community has generally moved away from legally binding agreements to deal with space stability and security, but a few continue to promote some form of treaty-based approach. These include Russia and China, which in February 2008 submitted the draft Treaty on the Prevention of Placement of Weapons in Outer Space and of the Threat or Use of Force Against Outer Space Objects (PPWT) to the international Conference on Disarmament. This proposed treaty would prohibit the testing or deployment of space-based missile defenses and space-based weapons more generally, even though no country is seeking such capabilities; it does, on the other hand, allow ground-based ASAT weapons, a capability that China tested in January 2007 (and most likely several times after that). The United States has repeatedly questioned the PPWT's lack of verification language, noting that U.S. policy will only allow for support of a space arms control treaty that is equitable, effectively verifiable, and beneficial to the national security of the participants. China and Russia released an updated version of the PPWT in June 2014, but it did not have any noteworthy changes. [108]

The United Nations also has the Committee on Peaceful Uses of Outer Space (COPUOS), which focuses solely on civil space issues and has historically striven to avoid discussions with security elements. However, more recently, this line has blurred in discussions within its working group on Long-Term Sustainability. Four expert groups, comprised of experts from around the world, were established in 2011 and tasked with examining several aspects of issues that would affect the long-term sustainability

of the space environment. They have put together nearly three dozen best-practice guidelines, which will be whittled down when they are presented to the larger COPUOS. Despite initial hopes that submission could take place in June 2016, this step most likely will be delayed, due largely to Russian intransigence.

Another official (but non-binding) effort to set the stage for a stable space environment is the guidance of the UN Group of Government Experts (GGE) on Transparency and Confidence-Building Measures (TCBMs) in Outer Space Activities. This group—advocated by Russia in 2010 and established by UN Secretary-General Ban Ki-moon the following year—was tasked with issuing a series of recommendations for improving space stability. The group's final report[109] defined TCBMs as "a means by which governments can share information with an aim of creating mutual understanding and trust, reducing mis-perceptions and miscalculations and thereby helping both to prevent military confrontation and to foster regional and global stability." It identified helpful space TCBMs that included information exchanges, voluntary visits, notifications of risk reduction activities, international cooperation, consultative mechanisms, and coordination. The report's solid guidelines will derive their strength from how well they are implemented, and it is too soon to assess the document's final effects on overall international security and stability. A joint session of the UN 1st and 4th committees took place in October 2015 per the GGE recommendations, but the meeting's execution was fairly wan.

Another international approach to space stability is the draft International Code of Conduct (CoC) for outer space activities, a proposed voluntary instrument that promotes the safe operation and utilization of space assets by building norms of responsible space behavior. After the European Union (EU) released a draft version in 2010 for international discussion, the document quickly faced criticism for the absence of many major space powers from its earlier planning. The proposed code was among the first EU foreign and security policy initiatives made possible by the 2009 Lisbon Treaty, and the bloc held a series of regional discussions on the CoC in an effort to compensate for its previous lack of inclusion. The first of these meetings took place in Vienna, Austria, in June 2012. This was followed by a May 2013 meeting in Kiev, Ukraine; a November 2013 gathering in Bangkok, Thailand; and most recently a May 2014 meeting in Luxembourg. U.S. policy formally supports the idea of "a" Code of Conduct, though not necessarily the proposed EU text, and the United States has affirmed its belief that the negotiating process is helpful.

Several concerns about the CoC persist. A number of major space stakeholders worry it was written to keep new actors from entering space, or to create costs that would make entry into space un-affordable for most. Meanwhile, advocates of a legally binding alternative are at odds with others who fear that a legal treaty would unduly limit the actions of legitimate space stakeholders. The potential inclusion of security issues in the document is yet another point of contention. The EU previously hoped to begin obtaining signatures for the CoC by the end of 2014,[110] but even a July 2015 meeting failed to answer numerous concerns shared by critics who doubted the document's fairness; such skeptics worried that the document was chiefly written by the West and consequently favored Western interests; moreover, they suggested that the draft's formulation outside of the United Nations meant it may not represent all viewpoints. In the end, the chair of the session, Sergio Marchisio of Italy, recommended that the UN General Assembly take up the CoC. As of April 2016, the CoC remains in limbo.

Domestic Considerations

In order to properly assess possible state responses during crisis, it is critical to understand the domestic constituencies of potential adversaries. Who truly speaks for the government, and who is an opinionated blogger without political connections? Who are the main decision-makers, and who are their primary audiences? By acting to improve transparency and helping outsiders to understand their thinking on space issues, governments can signal good intent and reduce the possibility of a crisis bubbling up or boiling over. States need not depend on the success of international discussions to demonstrate good intent; the release of data such as space budgets, plans, and policies can help to establish a baseline against which other states can compare their future behavior. A country can signal its approach to space in a publicly accessible national space policy, strategy, or white paper, which can serve as a reference in discussing priorities for its space program. Many countries do not do this, either to avoid the political process of putting one together—Australia's national space policy underwent years of review prior to its April 2013 release—or to maintain more flexibility in their approach to space.[111]

The United States also must be aware of its own domestic considerations, interests, and priorities in space. What does the country most value in its space architecture, and how can those attributes be ranked? While space stakeholders may not like to think of their respective capabilities as less important than others, not every space asset can be considered of "high value." Well before the onset of any crisis, policymakers must consider what support within the U.S. government would be required to take specific actions in space during a crisis. How much outreach and education is necessary prior to a crisis to expedite decision-making at crucial times?

Signaling Good Intent

States generally should focus on improving transparency to the greatest extent possible in order to signal good intent and to clarify and prevent misunderstandings. Because space assets can be wielded for innocuous and military purposes—sometimes simultaneously—it is impossible to predict a country's intentions through a simple examination of its space capabilities. Perception of intent is often an extremely subjective matter, shaped both by actions and by pre-existing relationships. In this respect, international cooperation and recognition of the inherent global nature of space can each serve to stabilize and strengthen relations. Just as responsible space behavior can signal good intent, reckless behavior in space can sometimes signal malevolent intent or encourage misinterpretation about the nature of a particular space asset. Blair and MacDonald discuss some of the challenges for space signaling in a later chapter.

Certain technical capabilities can signal good intent. Space situational awareness (SSA), for example, can help to improve understanding of other actors in space so that the worst-case scenario is not automatically assumed when a crisis situation appears to be brewing. SSA can help to indicate whether countries are acting responsibly in space, enabling operators to verify that others are following internationally established best practices and to "name and shame" violators. Currently, the U.S. military is the world's largest provider of SSA information.[112] While this information has been used to help avoid collisions on orbit, there are limitations to what it can accomplish and to its mission. A number of commercial and non-U.S. SSA programs and capabilities could amplify and verify data and information received and processed by the U.S. military. Utilizing other capabilities would improve overall coverage, as the current SSA network is predominantly comprised of radars in the Northern hemisphere. Such collaboration also would help make SSA information more comprehensive and dependable. In order for this cooperation to work, the U.S. military must be ready and able to accept input and contributions from non-U.S. sources, requiring a major shift in how the U.S. national security apparatus generally functions.

For activities of a dual-use nature, such as satellite servicing, certain technical steps could minimize or prevent misunderstandings that may otherwise lend themselves to awkward political situations. Such steps may include an advance announcement of a satellite servicing mission's intent and technical parameters, in-mission updates

on the relevant satellite's location, and an invitation for outsiders to confirm when the mission has concluded.

Political options to signal good intent are also available. By sharing relevant information within pre-existing relationships, space actors can attempt to exert a positive influence on the context within which an event is perceived. However, domestic legislative efforts can hamper international cooperation and the solidification of relationships with other space actors. Since 2011, for example, NASA and the White House Office of Science and Technology Policy have been forbidden from undertaking any bilateral effort with China on space issues. The restriction is based not on concerns about China's space program, but on worries about their treatment of religious minorities. As a result, the United States is limited in how it can communicate with one of the world's largest and most consequential space powers. Still, the first meeting of the U.S.-China Civil Space Cooperation Dialogue took place in Beijing in September 2015 with a goal to increase transparency on civil space issues. Additionally, the U.S. State Department and the China National Space Administration agreed to discuss space security issues as part of the broader U.S.-China Security Dialogue. Meanwhile, the United States could improve its approach to export control, which has added an inordinate amount of bureaucratic red tape to satellite exports. These restrictions have seriously limited the U.S. satellite industry's global outreach and impact, which in turn has limited the United States' ability to use space as a source of soft power.

Potential adversaries may shore up their relations ahead of a possible crisis by emphasizing their shared goals and acknowledging any divergent priorities. Certain differences on space policy are rooted in historical enmity: for example, developing countries sometimes suspect Western powers of seeking to regulate space primarily to their own benefit, essentially penalizing others for arriving late on the space scene. This suspicion skews perceptions, prompting developing nations to question whether the West submits its proposals for space cooperation in good faith. The varying interests of states also are partly attributable to differences in their space capabilities: while debris may be a major concern for an established space power, equitable access to space may be the highest priority for a nation at an earlier stage of space development. Even countries with relatively similar space capacities may have differing priorities. The United States, at discussions in Geneva, has described space debris as one of the largest possible destabilizing factors in space, while Russia (and, to a lesser extent, China) have appeared to assign that role to potential space weapons. This disparity of opinion affects international discussions and initiatives to stabilize the space domain.

By adopting shared or similar definitions of crisis stability and its components, major space stakeholders can reduce the likelihood that they will work at cross-purposes in a manner that precipitates crisis instability. The United States, for example, tends to perceive "threats" as potential military or other actions that adversaries may take deliberately to undermine its national security. Yet space commonly includes unintended phenomena, such as radio frequency interference, that could lead to a destabilized space environment if the United States assumed any consequent harm to its space assets to be a result of deliberate and malevolent action. In the harsh environment of space, satellites can stop functioning for reasons that include faulty engineering, space weather, solar flares (which can render space assets temporarily or even permanently useless), deliberate interference. If the United States prematurely attributed a halt in satellite broadcasts during a crisis to a deliberate attack, then political tensions with an adversary may worsen—perhaps unnecessarily.

Crisis stability is also shaped by preconceptions of actors. A country's activities in space will be viewed with suspicion if it is believed to have nefarious intent, but the state's space activities will not immediately be perceived as threatening if the nation is considered to be largely harmless. One such example is the Swiss experiment CleanSpace One, which aims to de-orbit an inactive satellite. Debris remediation typically raise political and security challenges, as any capability to de-orbit an inactive satellite could also be applied against an adversary's active satellite. However, CleanSpace One is not considered threatening for several reasons: it is an effort by a historically nonaligned state, it is a university project, and its target object was launched from the same nation, precluding liability concerns.

Finally, the blurring of numerous political distinctions in space has significant implications for the political environment and, consequently, for crisis stability. Space is no longer the domain of nation-states, as was generally the case during the Cold War. Numerous non-state entities now operate assets in orbit, and because commercial satellites now frequently carry military communications, no clear distinction exists between state and commercial space assets. In addition, space is now internationalized to an extent that one country's satellites may carry transponders that are critical to another nation's military communications, complicating any effort to anticipate consequences from deliberate interference with a country's space assets.

The overall space security and stability conversation must be expanded. When looking to strengthen the foundation of discussions for crisis stability, the United States must look beyond its traditional allies. Such pre-existing relationships can serve as a useful

springboard for further cooperation and discussions, but it is crucial to eventually include all major space stakeholders. The United States must ask what comes next: what is necessary for a stable, predictable space environment not just today, but also in the future? Incorporating non-traditional partners and emerging space actors will be a key element of this effort.

International Approaches to Fighting "the Four M's"

One modest but useful international approach to help make space a less destabilizing domain is through international dialogue. While it is difficult to resolve fundamentally conflicting national interests and priorities between adversaries, it should be possible to at least reduce risks of avoidable escalatory behavior resulting from "the four M's": miscalculation, misunderstanding, Murphy's Law, and Mother Nature.

Miscalculation and misunderstanding have played key roles in major conflicts over the last century and more, and they will continue to do so. Murphy's Law, or the tendency of improbable and unintended events to crop up when least expected, occurs at the national level as well. In a crisis, it is all too easy to attribute such events to malign adversary intent. The vagaries of Mother Nature that occur routinely in space prompt little thought of malign intent in peacetime, but they could too easily be attributed to an adversary during a crisis. It is reasonable to expect occasional space-asset outages caused by natural events, but such disruptions can appear suspicious or even threatening if they occur during a crisis. The key to addressing such space threats is to establish, maintain, and strengthen channels of communication for handling specific incidents and events. Countries can share information that helps to explain disruptive occurrences, and governments can coordinate joint action when appropriate. In addition, dialogue groups can address specific areas of contention between countries, helping participants to understand opposing perspectives. While such discussions rarely change minds, they enable each side to gradually grasp its adversary's frame of reference. In a crisis, such insight can help to screen out extreme explanations of adversary behavior that may otherwise catalyze worst-case assessments.

The United States has so far been unsuccessful in establishing a continuing government-to-government space dialogue group with China, which has proven reluctant to move forward despite its planned participation in a similar group on cyber-security, though there has been some recent progress.[113] The sides have been more active on space and cyber-security at the unofficial level, where Chinese and U.S. experts and former government officials have presented and exchanged ideas on space and larger strategic security issues, sometimes with current government officials acting as

observers or participants. These dialogues over time have helped to clarify important positions and reduce misunderstanding, as well as produce ideas for advancing the U.S.-China relationship. The author, who has participated in some of these dialogues with China, believes such exchanges are a worthwhile and cost-effective means to reduce misunderstanding and develop knowledge that may prove especially valuable in the event of a real strategic crisis in space or elsewhere. Such discussions can also help to pave the way for eventual direct government-to-government dialogue on space security, where crisis stability and crisis management likely would be important agenda items.

Crisis Stability, Signaling, and Communications in the Space Domain

ADM Dennis Blair, USN (Ret.), with Bruce MacDonald

The vastness of the space domain, coupled with the accelerating pace of national activities in space for commercial, scientific, and military purposes, provides many opportunities for both cooperation and confrontation. As the United States, China, and other countries depend more on space, especially in the military arena, the domain will assume an increasingly important role in potential crisis confrontation and conflict. Therefore, it has become more crucial than ever to understand possible sources of crisis escalation in the space domain, as well as approaches to better communicate with China and other potential space adversaries. The relative novelty of the security challenges of space, and worldwide inexperience in addressing them, are worrisome, and these challenges have no easy answers.

Space military activities in a crisis will not occur in isolation, and any assessment of actual space activities will depend heavily on actions in the conventional, nuclear, and cyber domains. While the following analysis focuses chiefly on the space domain, the authors recognize that external domains are a significant complicating dimension.

A fundamental issue for any country in crisis is the difficulty of signaling or interpreting whether a space activity is an entirely peaceful action, a defensive step taken in case the situation deteriorates, or an actual preparation for attack. Especially (though not exclusively) during a crisis or conflict, political leaders will examine potential actions with a view to how an adversary may interpret them, just as that adversary will attempt to understand the rationale and longer-term significance of any step taken. In situations of tension, the possibility for misunderstanding and miscommunication is very high.

Broadly, we can examine confrontation under three conditions: peacetime, crisis, and conflict.

Peacetime space activities of several types could generate tension:

- Jamming
- Satellite collisions
- Natural interference
- SAT and other counter-space testing
- Space-oriented exercises

Crisis behaviors, which are likely to be more diverse and threatening, include the above and several additional actions:

- A broad set of activities that can be grouped under the rubric of preparing the space battlefield
- Signaling and communications, both in the traditional sense as well as conveying more subtle information meant to influence adversary decision-making and deter or compel adversary behavior

Conflict behaviors in the space domain both the above steps and the following:

- Traditional military activities directly influenced by space
- Activities that have escalatory implications

Peacetime

In peacetime, low-level jamming and interference are not uncommon and are generally not escalatory, if they remain low-level. As noted earlier, some peacetime interference is even self-inflicted. Individual incidents can be cause for heightened awareness, but during peacetime, they are usually best handled through diplomatic channels when a jamming source is known. It is common knowledge that there is interference with ultra high frequency (UHF) military satellite communications during

peacetime. Often the source cannot be resolved, leading to suspicions that another country is probing U.S. communications. Such interference can occur during naval exercises, for example, though such incidents are usually one-off occurrences. The exercises are not disrupted, and such incidents actually add an unplanned realistic note to the proceedings. Still, questions for such incidents remain:

- What are the implications if dual-use (i.e., commercial/military) communications satellites are jammed?
- Can the source be identified?
- Are suspect countries cooperating in solving the problem, or are they obfuscating/prevaricating?
- Could a third-party proxy be carrying out the jamming on behalf of a country that is the real culprit?

A space power may suspect an adversary of deliberately producing an outage that in fact resulted from another source: an unintended satellite-satellite or satellite-debris collision, a solar storm, or another natural event. If several such unplanned incidents occurred in a short period of time, a state could misinterpret the coincidence as a sign of causation. Separately, if a U.S. adversary conducted kinetic or non-kinetic ASAT-related testing, the United States would need to determine the test's nature. Is it purely for developmental purposes, is it part of an exercise, or is it sending a deterrence signal? And who was in charge of the launch, national leaders or a cadre of over-enthusiastic space officers? Generally speaking, such a test would not be destabilizing as long as it targeted a country's own satellite. Jamming or laser dazzling a U.S. satellite would be more worrisome, though an isolated instance would likely be seen as little more than a nuisance. In addition, an isolated interference incident could provide useful intelligence about the jammer or laser being utilized, and such an occurrence would likely produce at least a modest increase in U.S. vigilance against possible repeated interference attempts.

Space Activities in Crisis Conditions

From the earliest stages of a crisis, intelligence activities will intensify on both sides, with satellite-based intelligence playing a key role. Likewise, military activities on both sides, including space activities, will intensify. Such steps are not, ipso facto, proof of an intention to go to war. Absent clear intelligence or another means to

understand the true nature of the preparations, each side will try to answer several questions, including:

- Is the other side merely taking precautions, or is it intent on striking first?
- Is the other side de-escalating, holding firm, or escalating?
- Are the space activities routine, preparatory, or intended to send a message? What message, if any, is being sent?

A key distinction will be whether any activities undertaken are reversible or irreversible, as most irreversible actions would essentially cross the boundary between crisis and actual conflict. It bears repeating that these events will not occur in isolation; events on the ground, where the crisis will most likely be centered, should be the most important factors in assessing the situation. Space activities associated with crisis behavior could easily magnify concerns and suspicions, as could increased adversary cyber activity.

Possible reversible space activities would include:

- Jamming of civilian communications satellites
- Jamming of military communications satellites
- Jamming of radar intelligence satellites
- Low-power, non-destructive lasing of imagery intelligence satellites
- Dispersal of kinetic ASAT launchers
- Preparation of ASAT launchers
- Cyber attacks on ground stations
- Possible irreversible space activities would include:
- High-power lasing of imagery intelligence satellites

- Destruction of LEO or GEO satellites by ASAT missiles
- Cyber attacks on space ground stations

Any space offense, especially in the transition from crisis to conflict, is part hostile activity and part signal. The challenge for the attacked country is to decipher the signal, understand the extent of the damage inflicted, and respond in a way that best advances the security interests of the attacked country, probably all in a compressed time-frame.

Participants in a crisis or early conflict also must exercise caution with respect to the unclear impact of various space actions. Actions that a combatant may believe to be reversible may cause more destruction than anticipated or expected; for example, a laser shot intended only to dazzle the optics of an adversary satellite may instead disable the optics, "destroying" the satellite from a functional perspective and making the action more provocative than intended. Furthermore, the attacker may not realize before the attacked party (or at all) that its strike disabled or destroyed the satellite, given the likely difficulty of space damage assessment. Thus even a proportionate response by the victim to the actual damage may appear to be an unwarranted escalation to the original attacker, which believed it had only dazzled the attacked satellite. This is just one example among many of how the "fog of war" can easily creep into the vacuum of space, with all that implies for crisis instability.

Space Activities in Conflict

It is entirely possible that at the earliest stages of actual conflict, hostilities would not yet have spread to space and space-related assets, beyond their roles in traditional military activities such as intelligence gathering and communications. Both sides could anticipate that an actual outbreak of hostilities would have a deterrent effect and lead to strenuous early diplomatic and other efforts to terminate hostilities quickly. The major question for each side to address is whether, and potentially how, to escalate the conflict into space. As neither side would likely relish the prospect of all-out conflict, given the economic and political-military stakes involved, any early escalatory moves into the space domain would most likely be modest and their objectives largely confined to traditional support of military activities and modest escalation to signal and convey deterrent and other messages.

The major challenge in the early stages of a conflict would be to ensure that the interpretation of any received message adequately reflects the sender's intention.

Given the novelty and relative lack of conflict experience in this new domain, there is a real danger that early signals could be misinterpreted. Early considerations for escalation into space would include:

- Reversible versus irreversible actions: irreversible actions would send a stronger message but be more escalatory; reversible actions would send a milder message
- Directed against civilian-only, military-only, or dual-use systems?
- Directed against less-costly or more costly satellites?
- Directed against nuclear early-warning or communications systems?
    - Defense Satellite Communications System (DSCS)
    - Nuclear Command and Control
- Orders given by national level authorities, or military commanders?
- Still possible to talk/negotiate about these questions, or damage too substantial to prevent further escalation in space?

In general, cyber attacks that do not destroy strategic-level infrastructure are probably less escalatory than space attacks because cyber attacks can be far more "granulated," or incremental, than space asset attacks, which are "lumpy" by comparison. In addition, space conflict would involve destroying or interfering with the physical assets of an adversary, possibly resulting in direct human casualties, whereas cyber attacks generally would not.

An incomplete but illustrative list of space activities, in ascending order of impact/threat, follows with comments.

Notional Crisis Action Scenarios

Amid all the uncertainties that will characterize a crisis situation, there is no single answer as to whether or not a particular step would be escalatory in a crisis. The impact of any action would depend on the nature of the crisis, what actions adversaries have already taken, whether the actions were taken in response to earlier adversary actions or marked a deliberate escalation, whether or not the actions were perceived

as escalatory, and many other factors. In theory, there is an ascending order of space activities in conflict by which to compare their relative seriousness, or the degree to which each would be threatening or destructive. A major problem is that state assessments of each activity's seriousness may differ, potentially causing miscommunication to be a significant problem. It nonetheless is useful to review credible space and space-related actions and note their possible impact in a notional crisis situation. The actions chosen below are not authoritative but are intended to illustrate a general hierarchy. They fall into the following broad categories:

- Signaling
- Raising the alert status
- Battlefield preparation/defensive actions, such as moving equipment around
- Offensive action – reversible
- Offensive action – irreversible
- Tactical or limited war-fighting
- Strategic attack

In signaling, it is difficult for either the initiator or the recipient to distinguish whether an action reflects communication of intent or an actual hostile degradation of capability, or some measure of both. The cumulative effect of space signals also depends on target resilience; some aged systems in space may prove less resilient than anticipated. China is unlikely to know the precise effect of jamming or lasing on certain targets due to its relative inexperience in such matters, and it is difficult to believe that the United States would be much better in doing so. For a number of reversible steps, factors such as the difficulty of carrying out attack assessment mean, at a minimum, that there will be tremendous uncertainty about the effects of actions in space.

The following Table 2 presents more specific plausible actions affecting space assets, followed by comments. Again, this is hardly an exhaustive list, and the reader is encouraged to add his or her own.

Table 2. Actions Affecting Space Assets

Action	Comments
Localized GPS/Other Jamming	Worrisome, but probably not escalatory if kept localized. Could lead to jamming in response.
Regional GPS/Other Jamming	More worrisome and almost certain to lead to jamming or some other response.
Reversible Attacks on Military SATCOM	A response would vary with the scale of the original action. Which circuits? Tactical or strategic? Military only or military/commercial? Even if isolated, action of this nature would cause concern and is likely to prompt a response. If not isolated, this action would be escalator.
Major Repositioning of Orbiting Satellites	Depends on which satellites and what likely intent. Its very unusualness likely to stimulate concern and responsive measures from other side.

Table 2. Actions Affecting Space Assets *(continued)*

Action	Comments
Attacks on PNT systems[114]	Collateral damage? Risks of retaliation?
Jamming Radar Intelligence Satellites	Implies a desire to deny information to an adversary, with all that could imply. This step is likely escalatory and not minor, even if it is reversible.
Dazzling Intelligence Satellites	Implies desire to deny information to adversary, with all that could imply. This step is likely escalatory and not minor, even if it is reversible, because it implies a serious threat to negate this crucial source of intelligence information, a step not to be taken lightly.
Isolated flushing of individual ASAT TELs w/o missiles	If consistent with other activities suggesting an exercise, not escalatory. Otherwise worrying.

Table 2. Actions Affecting Space Assets *(continued)*

Action	Comments
Attacking a satellite of one's own	A dramatic signal of willingness to escalate direct attacks against an adversary without directly damaging that adversary's infrastructure.
Conventional or special forces attacks against space ground facilities	U.S. long-range precision strikes. Chinese and proxy sabotage attacks. Highly escalatory.
Attacks on nuclear C3 systems	An attack would be highly escalatory and suggest potential for a nuclear attack (or that an adversary fears such an attack and is pre-emptively degrading adversary capabilities to launch one).
Flushing SC-19/ASAT TELs from bases	Escalatory.

Table 2. Actions Affecting Space Assets *(continued)*

Action	Comments
Cyber attacks on key satellite ground stations	Can they be precise? How sustainable?
Attacking conventional communication satellites	An attack on just one or two satellites would be escalatory, and could signal that an adversary is on the verge of a much larger space asset attack. A larger number of attacks would represent a major attempt to disrupt communications with regional military commanders.
Attacking Imaging MILSATS	Attacks can be reversible or irreversible. Irreversible attacks are far more escalatory. Either would risk comparable retaliation.
Attacking DSP/SBIRS LDS	This and other attacks on strategic nuclear infrastructure would suggest preparation for possible nuclear attack. This highly destabilizing and escalatory action would threaten to cross the nuclear threshold.

Discussion

With the exception of modest, reversible space actions that may be useful for signaling, the chief objectives of action in the space domain would be military rather than diplomatic. Therefore, action beyond a low level would create strong military imperatives to attack the ground- and space-based space systems of an opponent in an escalating crisis or early-stage conflict, especially one between the United States and China. Signaling intent can be very important, but particularly in space, there are serious dangers associated with conducting attacks that are primarily intended to send a message. The physical effects of more substantial space attacks—in terms of collateral damage, secondary effects, and civil impact—are neither well known nor well understood. When the highly interconnected nature of cyberspace is taken into account, these uncertainty concerns are magnified further. Overhanging these considerations will be the threat of rapid escalation if a country believes it has more to gain, or less to lose, if it escalates first and quickly, as discussed earlier.

Signaling one's adversary in a crisis or early in a conflict is fraught with potential danger. The risk of miscommunication is very high, opportunities for dialogue are few, and even dialogue itself can suffer from misunderstanding. Yet any action taken in such circumstances, even if it is for purely military purposes, conveys an implicit message about intent and thus has an important political dimension. Under these circumstances, diplomacy would benefit from the experience and background of prior strategic dialogue with potential adversaries on space and on interactions between the space and cyber domains. Just as war games give participants a way to consider challenges that could occur in real life, dialogue can help to reduce, though not eliminate, the chances for misunderstanding in a crisis. While not a perfect solution, such dialogue, and the channels of communication that can be opened up, could prove highly useful in a crisis.

This has been just a brief overview of a very complex problem that requires much more attention and analysis. Achieving and maintaining a highly resilient space infrastructure, if possible, would probably do much to preserve stability in space by reducing the expected benefit from counter-space attacks. On the other hand, resilience could paradoxically worsen stability concerns if it led to "moral hazard" behavior by the more resilient power, which could be led by its more resilient infrastructure to believe it had less to risk. On balance, though, it appears that greater stability would be the net effect of a resilient space architecture. A stabilizing outcome appears even more likely if resilience is not exclusive to just one space power's architecture. Whether or not space resilience can be achieved, and whether or not such resilience would be

stabilizing, establishing and maintaining dialogue between U.S. and Chinese civilian and military counterparts on space should be considered an essential stabilizing ingredient of the Sino-U.S. relationship going forward. Such dialogue will never eliminate the risk of unintended major conflict in space, much less intended conflict, but it can help to reduce chances of misunderstanding and miscommunication, as well as the ever-present threats posed by Murphy's Law and the random effects of Mother Nature.

OBSERVATIONS, CONCLUSIONS, AND FINDINGS

There is little doubt that the nature and characteristics of military space, and its increasingly essential role in the conventional forces domain, make strategic and crisis stability in space more important and less certain than ever before. The challenge for U.S. and allied decision makers, and for other space powers such as China, is to help shape a space domain with policies, hardware, software, and architectures that minimize the likelihood that any future crisis, in space or in other domains, will escalate due to the characteristics and features of the space domain itself. Ideally, the space domain would even serve a de-escalating role and prevent conflict from escalating into space. However, the obstacles to achieving anything close to this ideal state are formidable.

Observations on the Strategic Landscape of Space

While all may wish otherwise, there seems to be no escaping the fact that deterrence plays an important role in the maintenance of stability in space, though that role is far from solitary. An essential issue for U.S. policy is how to best deter an attack against U.S. and allied space assets. Unlike during the Cold War, when the United States and the Soviet Union each could access public information about the other power's strategic nuclear assets (though mostly from U.S. sources), today's publics have little qualitative, much less quantitative, information about one another's offensive space weapons. This gives rise to a fundamental question: how can the United States deter adversaries, and assure its friends and allies, when it largely conceals the forces, doctrine, and training behind its deterrence and assurance messages? (China maintains similar secrecy in these areas.) While some forces are possible to observe using traditional surveillance and intelligence methods, others are more difficult to monitor. This same problem exists to a far greater extent for cyberspace, where offensive capabilities are undetectable except through an extraordinary intelligence coup. Virtually no public debate has taken place on this question, though it likely has been discussed within the government. What are the advantages and disadvantages of withholding information concerning U.S. space and cyber offensive capabilities, and how does secrecy on these matters improve or worsen stability and deterrence? What types of

offensive space capabilities should the United States seek? At what levels? And, most importantly, to what purpose?

While nuclear weapons completely reshaped the landscape of great power dynamics, they retained some familiar elements of great power strategy. Nuclear weapons could be counted, and their effects, though terrifying, were also quantifiable to an extent. As U.S. and Soviet officials developed familiarity with the implications of various weapon types, their understanding of these strategic realities led to dialogue and ultimately to agreements that limited competition in the nuclear domain. Yet none of these conditions apply to space or cyberspace, where weaponry can be highly effective and produce effects that are difficult to predict, given the degree to which both domains are connected with the conventional and nuclear domains. Counter-space capabilities are difficult to count or compare in detail, their substantial indirect effects are difficult to quantify, and their inventories are never discussed in public. Their arsenals, which include cyber-based counter-space capabilities, are largely invisible. Over time, the two Cold War superpowers developed venues to discuss nuclear issues, including but not limited to arms control. There is today an aching need for discussion of space and cyber dynamics and crisis stability issues, if only to develop a common language and understanding of the issues involved, as well as to provide each major power with insight on how the other powers understand these concepts and view opportunities and potential pitfalls from space and cyber weapons. It is unlikely that such dialogues, at either the government-to-government or experts-to-experts level, can resolve most or even a sizable portion of the many issues that the United States and China face in the military space arena. Such dialogues can, however, reduce misunderstanding, strengthen and clarify perceptions of how other countries perceive important space issues, and in some cases permit modest, incremental progress that can permit discussion of more fundamental issues. A journey of a thousand miles begins with a single step.

The military and commercial value of space assets is in the information they either generate or transmit. Thus space crisis stability and deterrence can be seen as an important dimension of the larger issue of cyber conflict. Viewed from this perspective, space conflict seems unlikely to remain purely in the space domain except at the very lowest level of hostile activity (e.g., jamming an individual satellite).

Beyond modest lower-cost defenses to address relatively unsophisticated space and cyber threats, the advantage that offense currently enjoys in space means that effective space defense is less concerned with actively defending space assets than with providing system resilience, graceful degradation, alternative backup systems, and other means to preserve core SEIS capabilities in a conflict. This is not unlike the role of sea-based nuclear weapons in the nuclear domain, where nuclear-armed submarines are not actively defended but are simply quite difficult to attack and defeat. (It should be noted, though, that resilient space assets are not likely to be as robustly survivable as sea-based nuclear weapons.)

Military espionage has been a feature of human conflict since the dawn of civilization, and space espionage has followed in its trail since the start of the Space Age and the early exploits of the U.S. Corona program. Cyber espionage has already become a part of the intelligence domain, and it seems unlikely to be viewed as destabilizing except in the most unusual of crisis circumstances.

Beyond lower-level threats from non-peer countries, it appears unlikely that a country will seek to engage in any space offense against the United States in the absence of war, except as an isolated non-damaging test (e.g., China shined a laser on a U.S. reconnaissance satellite in 2006[115]) or to send a signal in a crisis situation by demonstrating the capability. Unlike in the cyber domain, where non-state actors can conduct fairly sophisticated attacks, significant hostile actions against space assets, with the important exception of cyber attacks, are almost the exclusive province of nation-states.

As space architectures are currently constituted, strong incentives exist for escalation in both space and cyberspace. There are major advantages to striking first in both domains: offensive capabilities are intact, adversary defenses are probably lower, and the attacker enjoys the element of surprise. In peacetime, these incentives are easily outweighed by all the drawbacks of an attack: the threats to national economic and physical well-being, the chance for unanticipated and disastrous repercussions, the risk of political upheaval in a one-party state, and many more. In the context of a crisis, however, these calculations may change. A country fearful of an adversary first strike may itself initiate an attack not because it wishes to in the strictest terms, but because it sees launching a first strike as preferable to potentially being a victim of one. Furthermore, rapid escalation affords the major benefits of maximizing surprise and weapons effectiveness. Both incentives bode quite poorly for crisis stability in space.

Counter-space capabilities and cyber weapons are fundamentally different from nuclear weapons in many respects, but all share at least one characteristic in common: they are not just "one more weapon in the arsenal." Their special qualities demand recognition and respect, and decisions involving their use should be taken with great

care, recognizing that they may place at stake the vital national interests of the United States, and of adversaries. Better understanding the strategic landscape of space, and cyberspace, is an essential twenty-first century priority.

At least five characteristics of the space domain add substantial uncertainty about crisis stability going forward:

- *Rapid space/cyber technological change*. The evolution of technologies across the board makes it difficult to project what the future space environment will look like or how it will "behave." Capabilities and behaviors may be entirely different in the space environment of 2030 compared to today, given the accelerating development of new space and cyber technologies and capabilities.

- *Unpredictable cross-domain interdependencies*. As the world becomes ever more interconnected, the space and cyber domains are growing increasingly enmeshed with the traditional military domains of land, sea, and air, and with economies around the world. As a result, the difficulty of predicting effects from inactivating or destroying space assets is constantly increasing, which boosts the likelihood that an attack could cause an inadvertent level of destruction and consequently trigger a stronger-than-expected retaliation in space and/or other domains.

- *Major threat uncertainty*. In addition to uncertainty over how adversary space threats will evolve, it is becoming more difficult to estimate what offensive space forces an adversary even has. The launcher for China's kinetic ASAT weapon is quite similar to those of other deployed Chinese ballistic missiles, and more exotic space weapons also are not easily distinguished. Moreover, it is exceptionally difficult to determine the extent to which offensive cyber capabilities may target space infrastructure, and understanding the potential effectiveness of cyber weapons on space assets is an even greater challenge.

- *Inexperience operating in the strategic space landscape*. From a space conflict perspective, space is a new domain of operations; even the United States, which possesses more space experience than any other country, has very limited experience when it comes to conflict in space. This lack of experience, especially for relative space newcomers such as China, means that mis-perception and over-reaction to events are particularly likely in the space domain, further aggravating the problem of crisis stability in space. Indeed, China's inexperience in recent actual conflict of any kind only underlines this issue.

- *Persistent Uncertainty About Attack Effects*. Ongoing rapid change in both the technology and the architectures of space and cyberspace, coupled with the ever-growing interconnectedness among infrastructures of advanced economies, means that major space powers will likely never have much confidence that they can predict the impact of major strategic space or cyber attacks, no matter how much their modeling techniques advance. Simply mapping the potential impact of attacks on today's space and cyberspace architectures would be difficult, given their current interconnectedness. Yet the real challenge is exponentially greater in at least two dimensions: the technology continues to advance rapidly, and inventive designers develop new ways to manage complex systems that inevitably result in greater component integration and thus more interconnectedness. The dawning of the era of the "internet of things" will almost certainly multiply these interdependency effects Attempting to predict effects from potential space and cyber attacks would not be unlike trying to predict the weather months in advance; ever-changing conditions and complexity would make either endeavor virtually impossible. To the extent that these uncertainties are appreciated and understood, they should further enhance risk aversion among rational adversaries going forward. In addition, space is an offense-dominant environment as it is currently configured, with architectures comprised of a smaller number of highly complex and relatively vulnerable satellites. It is much easier to attack even high-value space assets than it is to defend against attacks, giving offense a major advantage.

Conclusions

1. T*he single most stabilizing step the United States can take in space is to develop a far more enduringly resilient space architecture that can absorb a first strike and still deliver acceptable performance that allows U.S. military forces and decision-makers to receive the information they need.* A combination of highly disaggregated satellite architectures coupled with aeronautical and other backup systems appears to offer great promise to this end. High-performance satellites that are large and costly will likely still have a role to play, but this role must become smaller in the future unless the United States wants to place itself on the wrong side of technological history and jeopardize its security interests. Of greatest importance are space assets that protect U.S. nuclear deterrent capabilities.

In addition, backup U.S. non-space systems that are not directly threatened by adversary space offense would further reinforce crisis stability.

2. *Some U.S. space offense is needed.* Some level of space offensive capability beyond what is intrinsically available to the United States through its BMD capabilities would help to strengthen stability in space, but pursuing such capabilities would involve a "Goldilocks" element of uncertainty. The United States should not seek so much offensive space capability as to trigger major offensive buildups by potential adversaries, as that dynamic would create exactly the kind of instability that Washington should seek to avoid. Any U.S. offensive space capabilities must be survivable, which almost certainly requires them not to be based in space. The United States may not need dedicated offensive space capabilities to deter attacks on its space assets, strictly speaking, due to its robust military capabilities in other domains. The relevant question is not whether the United States needs such capabilities, but whether having them would be a net benefit to U.S. security interests. While such offensive capabilities may not be needed in a strict sense, there appear to be important benefits to having at least some significant offensive space capability, if for no other reason than to prevent the United States from being forced into a major casualty-producing response to a significant but bloodless adversary strike against U.S. space assets. Few crisis or early-conflict actions are as escalatory as one side waving a "bloody shirt" created by an adversary's actions. Jordan's military offensive reaction in early 2015 to its pilot being burned alive by the Islamic group ISIS joins a vast company of similar reactions in history. Space deterrence currently appears far more likely than nuclear deterrence to fail in a crisis or conflict, for which the United States must be prepared. Offensive space capabilities could help the United States to contain any conflict within a single domain and to achieve the stabilizing goal of minimizing direct human casualties. In addition, the development of at least a limited offensive space capability would strengthen U.S. deterrence, providing a measure of reassurance to the many allies that depend on U.S. deterrent capabilities for their security. However, any use of such capabilities in conflict should be selective and not indiscriminate, given the risks of both horizontal and vertical escalation.

3. The United States must *expect maintaining space resilience to be an ongoing struggle*, not a simple one-shot accomplishment, and this recognition must be reflected in both budgeting and military planning. Given the importance

of space to U.S. conventional force superiority, steps to reduce U.S. space vulnerability are unlikely to prompt a country such as China to simply stop seeking countermeasures to U.S. space capabilities. Rather, there is likely to be a measure-countermeasure space competition not unlike the submarine/anti-submarine warfare competition of past and present years. The United States must recognize that maintaining space resilience will probably be an ongoing struggle against adversaries that will try to develop countermeasures to a resilient architecture, and it must plan accordingly.

4. The United States must also recognize that *as Chinese space power grows, it too will seek a more resilient space architecture*, with all that implies for maintaining credible U.S. space control capabilities. In this regard, China (and perhaps Russia) will present the United States with the very challenge that Washington will seek to impose on adversaries. In addition, the United States will need to weigh potential benefits from seeking to deny such resilience to China and others against the implications of such efforts for crisis stability, and strategic stability, in space.

5. *The United States, China, Russia, and other developed countries should see a common interest in avoiding strategic space and cyber conflict.* Such conflict would threaten economic and other destruction that would cripple those countries and most others in a way the world has never experienced, especially when indirect effects are taken into account. A country like China, which has achieved a level of economic security unknown in its history, should be especially reluctant to risk its past and future progress on any serious plan to engage in major strategic space, and cyberspace, warfare. The cost could rival that of a strategic nuclear conflict, though without the climate impacts. China's demographic and other challenges, which include a need to mitigate political unrest through healthy economic growth, would likely introduce a strong note of caution into the behavior of the CCP's Politburo in a crisis. Two very large (and nonexclusive) caveats to this assessment are: 1) the possible behavior of China (or another space near-peer) if it feared that failure to act would risk the fall of its government, and 2) the Politburo's uncertain ability to maintain tight control over the PLA, which may not have the same world-view in a serious crisis or active conflict. China's lack of a National Security Council-type body, and the PLA leadership's relative isolation from non-PLA issues, do not inspire confidence.

6. *Given that the United States obtains more benefit from space than any other country, it should exercise great caution in considering the first use of offensive space capabilities.* If offense predominates in space, why should the United States engage in an arena where it will likely be the bigger loser in a conflict with a space near-peer? If the adversary is not a near-peer, using offensive space capabilities probably would provide relatively little incremental benefit and therefore not be necessary: non-space means would likely be sufficient to defeat the opponent. In addition, given the presumptive U.S. interest in reinforcing a norm of non-use of counter-space capabilities, it would make little sense to violate this norm to defeat a much weaker adversary.

7. *Unlike nuclear crisis and nuclear combat, where any use of nuclear weapons almost inevitably would escalate to all-out nuclear war, the situation in a space and/or cyber conflict would be more muddled.* Even at its worst, all-out space and/or cyber war appears unlikely to produce as many casualties as all-out nuclear war. That said, there could still be substantial indirect casualties from economic damage, and the military consequences of a SEIS outage would likely be very substantial. Furthermore, an all-out space and/or cyber conflict would likely spread to more traditional domains, which would certainly affect crisis and intra-war decision-making.

8. *Until the United States can either achieve a robustly resilient space architecture, a survivable second-strike offensive space capability, or both, there is some prospect that risk aversion can play some role in providing some space stability in serious crisis or early conflict conditions.* However, any resultant stability is unlikely to be robust and could well fail at an inherently unknowable stage.

9. *In the early stages of conflict, there will always be a temptation to escalate offense in space, if practical, from very limited tactical objectives to achieve larger objectives. The perceived benefits of such escalation must always be weighed against the risk that such escalation could grow unstable,* with no obvious signposts along the way that unstable escalation has begun. The danger is that military specialists on either side may overlook key strategic considerations, which makes broader input into crisis decision-making a must.

Findings

Place Priority Emphasis on Resilient Space Architecture Development. The single biggest challenge to crisis stability in space is the major incentives that exist under current architectures to strike first and strike hard against U.S. space assets. This both weakens U.S. ability to deter such attacks and places vital U.S. security interests in space at serious risk. Developing greater space resilience and other backup approaches to securing U.S. assets in space and on earth will pay major dividends in crisis stability, deterrence, and effectiveness of U.S. military forces and decision-making at senior leadership levels. Particular attention should also be paid to long-endurance, high-altitude UAVs that would operate in a completely different physical domain from space and thus buttress U.S. SEIS capabilities, at least in certain applications. Satellite self-defense capabilities should be explored for their feasibility.

Develop Offensive Counter-Space Capabilities Consistent with U.S. National Space Policy for Primarily Deterrence Purposes. In conjunction with a more resilient space architecture, the United States would on balance benefit from possessing offensive space capabilities that are sufficiently survivable to deter other space powers from believing they could obtain major "bloodless" military advantages while forcing the United States to respond either with major casualty-producing steps or possibly with cyber actions of far less certain effectiveness. Such offensive capabilities should be highly survivable and able to deliver temporary and reversible effects that can negate adversary space satellite capabilities. Along with such capabilities, the United States should adopt an approach similar to the "dual-track" formula that has informed initiatives such as the Reagan administration's simultaneous pursuit of nuclear stockpile modernization and talks to eliminate intermediate-range nuclear forces. The objective in this case would likely not be an outright ban on space offense, but verifiable restrictions that would enhance stability and security. Such an approach would couple the development of offensive capabilities with a push for international guidelines and verifiable agreements to enhance U.S. and international security interests in space, such as space operations "rules of the road" and a ban on testing or deploying major debris-producing space offensive capabilities, among others. Pursuing space offense without a corresponding diplomatic initiative would be unwise and would forgo an opportunity to enhance U.S. and world security interests through modest but useful diplomatic steps to reduce opportunities for inadvertent escalation.

Strengthen the Taboo on Attacking Nuclear Force-Supporting Infrastructure. Actions that indicate any interest in targeting the key space infrastructures that support nuclear forces would be extremely destabilizing, as they would suggest that preparation for nuclear conflict is under consideration, whether or not it actually was. Likewise, cyber actions that target supporting infrastructure of major adversary nuclear forces would be highly destabilizing. Precisely because of their destabilizing nature, such actions

would be attractive to some non-state actors, and decision-making and planning should reflect this possibility. The non-identical nature of space assets among potential adversaries is also a consideration that affects calculations and judgments; for example, the United States places high value on its missile warning satellites (SBIRS, DSP) while China presently has no comparable satellites.

Some Chinese sources and statements suggest that conventional, non-nuclear U.S. strikes on Chinese nuclear forces such as ICBM silos, or strikes that produce effects similar to weapons of mass destruction could justify a Chinese nuclear response. Beijing to date has been ambiguous on this point, usually just repeating its standard assertion that there will be "no first use of nuclear weapons" by China. China's 2012 Defense White Paper excluded this language, surprisingly, and the author's unofficial discussions with Chinese officials, academics and others have reinforced the possibility that Beijing may have loosened its no-first-use perspective. [116]

Encourage Greater U.S.-China Dialogue on Space. In a crisis, the single most important non-military option is to dialogue with the adversary country. The effectiveness of this step will be greatly aided if related discussions have already taken place, helping players to become familiar with each other and the issues involved. While dialogue should be initiated in any case during a crisis, a relevant communications channel would be far more valuable if it were already in place. This is one argument made for discussions among major space powers on establishing a space code of conduct or "rules of the road." The United States and China should, at a minimum, commence an ongoing space dialogue on a government-to-government basis. The talks would aim not to resolve all differences, but to reduce misunderstandings, establish communication channels for use in an actual crisis, and develop each country's familiarity with the other side's approach to the issues. Such talks need not be a zero-sum game: both sides stand to benefit. In fairness, it must be said that China has rebuffed U.S. proposals for such talks on numerous occasions. China's rejections could be based at least in part on anger at being barred by Congress from civilian interaction with NASA. This space dialogue should expand to include other countries as appropriate, but China should be the top priority. In particular, emphasis should be placed on encouraging greater senior-level military-to-military space dialogue. The United States has long advocated such dialogue, and China should be more forthcoming in this area.

Take Steps to Better Exploit Risk Aversion and Uncertainty. Risk aversion will play an increasingly important role in crisis stability as the U.S. and Chinese economies grow more interdependent and more reliant on space and cyberspace. As both sides better

understand the unpredictability of potential cascading impacts from a larger-scale space and cyber attack, such strikes may gradually become considered relatively taboo, as nuclear attacks are viewed now. There are already indications that China, with its growing economy, is slowly developing more appreciation for the dangerous unknown consequences of such attacks.

Consider a No-First-Use Policy for Kinetic Offensive Counter-Space Capabilities. The substantial use of direct-impact kinetic ASAT weapons by either or both sides of a conflict should be avoided, as such use could wreak tremendous and long-lasting damage on key orbits in space with major economic and other consequences. The United States should give serious consideration to announcing a no-first-use pledge for such weapons. This commitment would likely have little impact on U.S. offensive capabilities and would put China on the diplomatic defensive, as it appears such weapons are or soon will be part of its arsenal. A U.S. no-first-use pledge for kinetic offensive counter-space capabilities could be followed by a multilateral prohibition on tests of such weapons, with care taken to prevent any loopholes.

Conduct More Extensive Crisis Games to Better Understand Space Crisis Dynamics. The U.S. Department of Defense should expand its space "war-gaming" exercises to include a full suite of space-oriented "crisis games" with the objective of gaining deeper insights into the behavior of the United States, China, allies, and others in a space crisis context, either apart from war games or as an important adjunct to them. Specific focuses could include the impacts of different kinds of signaling in a crisis, the role of uncertainty, space-cyber interaction, and techniques to de-escalate in a crisis or in the early stages of actual conflict.

Consider Ending the Reluctance to Reveal the "Fact of" Offensive Counter-Space Capabilities. The United States and China both maintain a studied and firm position of evasion on the subject of offensive space capabilities, officially neither confirming nor denying possession of such capabilities. As this report has sought to show, there is much to be said in favor of reticence in revealing details about these capabilities. Capability uncertainty, coupled with demonstrated space (and cyber) technological prowess, enhances adversary uncertainty about one's offensive capabilities and encourages risk-averse behavior in a crisis. However, encouraging a risk-averse mindset requires the release of at least a small amount of information about one's offensive space capabilities, even if it is only an acknowledgment that one has such an arsenal. The United States took analogous action in 1978 by confirming its possession of imaging satellites, ending years in which it had refused to directly address one of its worst-kept

security secrets.[117] Pointing to U.S. satellite jamming capabilities, such as the unclassified Air Force Counter Satellite Communications System (CSCS), is one option at least worth considering.[118] Effective deterrence requires that potential adversaries have some awareness of the challenge they would confront.

We as a nation go forward into an ever more complex and interdependent world full of promise as well as pitfalls. Understanding and adapting to the constantly changing contours of the strategic landscape of space that await us will be a major challenge that this country must address.

GLOSSARY

ASAT	Anti-Satellite (weapon)
ASBM	Anti-Ship Ballistic Missile
BMD	Ballistic Missile Defense
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
CCP	Chinese Communist Party
CMC	Central Military Commission, China's most senior national security body
CoC	Code of Conduct
COPUOS	Committee on the Peaceful Uses of Outer Space (United Nations)
CSCS	Counter Satellite Communications System
DARPA	U.S. Defense Advanced Research Projects Agency
DEW	Directed-Energy Weapon
DSCS	Defense Satellite Communications System
DSP	Defense Support Program (Missile early warning satellite system)
EMP	Electromagnetic Pulse
GEO	Geosynchronous Earth Orbit
GGE	Group of Government Experts (United Nations)
GPS	Global Positioning System
GSSAP	Geosynchronous Space Situational Awareness Program (Air Force)
ICBM	Intercontinental Ballistic Missile
IED	Improvised Explosive Device

INF Intermediate-range Nuclear Forces

ISR Intelligence, Surveillance, and Reconnaissance

LEO Low Earth Orbit

MOU Memorandum of Understanding

NASA National Aeronautics and Space Administration

NATO North Atlantic Treaty Organization

ORS Operationally Responsive Space

PLA People's Liberation Army, China's armed forces

PBSC Politburo Standing Committee

PNT Pointing, Navigation, and Tracking (e.g., GPS, Beidou)

PPWT The Treaty on Prevention of the Placement of Weapons in Outer Space and of the Threat or Use of Force Against Outer Space Objects (proposed)

PRC People's Republic of China

SATCOM Satellite Communications

SBIRS Space-Based Infrared System

SEIS Space-Enabled Information Services

SLBM Sea-Launched Ballistic Missile

SM-3 Standard Missile 3, a U.S. missile defense interceptor

SSA Space Situational Awareness

SSBN Fleet Ballistic Missile Submarine, a nuclear submarine with ballistic missiles

TCBM Transparency and Confidence-Building Measures

TT&C Telemetry, Tracking and Control system, which provides vital communications to and from a satellite. TT&C is the only way to observe and control the spacecraft's functions and condition from the ground.

UAV Unmanned Aerial Vehicle

USIP United States Institute of Peace

X-37B An Air Force experimental orbital test vehicle program to demonstrate technologies for a reliable, reusable, unmanned space test platform base on NASA's X-37 design. The unmanned vehicle is designed for vertical launch to low Earth orbit where it can perform long-duration space technology experimentation and testing.

NOTES

[1] See, for example, Grego, Laura. "A History of Anti-Satellite Programs." Union of Concerned Scientists, January 2012. http://www.ucsusa.org/sites/default/files/legacy/assets/documents/nwgs/a-history-of-ASAT-programs_lo-res.pdf. Also see Weeden, Brian. *"Through a Glass, Darkly."* Secure World Foundation, March 2014. http://swfound.org/media/167224/Through_a_Glass_Darkly_March2014.pdf, March 2014.

[2] The contributors included current (2016) Secretary of Defense Ashton Carter.

[3] Carter, Ashton, Desmond Ball, Hans Bethe, Bruce Blair, Paul Bracken, Hillman Dickinson, Richard Garwin, et al. *Crisis Stability and Nuclear War.* American Academy of Arts and Sciences and Cornell University Peace Studies Program, January 1987, 44-47.

[4] White House. *National Space Policy of the United States of America.* June 28, 2010. http://www.whitehouse.gov/sites/default/files/national_space_policy_6-28-10.pdf.

[5] U.S. Air Force. *Air Force Doctrine Document 3-14: Space Operations.* June 19, 2012, 21. http://static.e-publishing.af.mil/production/1/af_cv/publication/afdd3-14/afdd3-14.pdf.

[6] Perry, William, James Schlesinger, Harry Cartland, John Foster, John Glenn, Morton Halperin, Lee Hamilton et al. *America's Strategic Posture: The Final Report of the Congressional Commission on the Strategic Posture of the United States,* U.S. Institute of Peace, 2009, 71. http://www.usip.org/sites/default/files/America's_Strategic_Posture_Auth_Ed.pdf.

[7] White House. *Fact Sheet on U.S. Space Policy.* https://www.whitehouse.gov/the-press-office/fact-sheet-national-space-policy, June 28, 2010.

[8] *The Washington Post* attributed this data to the U.S. Organization for Economic Cooperation and Development. See Ferdman, Roberto. "The U.S. still spends more on space than every other country—combined." *Washington Post,*

October 25, 2014. https://www.washingtonpost.com/news/wonk/wp/2014/10/25/the-u-s-still-spends-more-on-space-than-every-other-country-combined/.

[9] White House. *U.S. National Space Policy,* 2006. http://www.whitehouse.gov/sites/default/files/microsites/ostp/national-space-policy-2006.pdf.

[10] White House. *National Space Policy of the United States of America,* 2010.

[11] Department of Defense Fact Sheet (2011):"DOD Strategy for Deterrence in Space; http://archive.defense.gov/home/features/2011/0111_nsss/docs/DoD%20Strategy%20for%20Deterrence%20in%20Space.pdf

[12] National Security Space Strategy, January 2011, https://fas.org/irp/eprint/nsss.pdf

[13] National Aeronautics and Space Administration. "Space Debris and Human Spacecraft," September 26, 2013. http://www.nasa.gov/mission_pages/station/news/orbital_debris.html.

[14] Aerospace Corporation, Crosslink Magazine, "A Space Debris Primer," December 10, 2015.

[15] Weeden, Brian. *Iridium-Cosmos Collision Fact Sheet*. Secure World Foundation, 2012. http://swfound.org/media/6575/swf_iridium_cosmos_collision_fact_sheet_updated_2012.pdf.

[16] U.S. Department of Defense, Directorate of National Intelligence *National Security Space Strategy*, Unclassified Summary. January 2011, 2. https://fas.org/irp/eprint/nsss.pdf.

[17] Freedberg, Sydney J. Jr., *Breaking Defense*, December 2, 2015, http://breakingdefense.com/2015/12/us-jammed-own-satellites-261-times-in-2015-what-if-an-enemy-tried/.

[18] U.S. Department of Defense, Directorate of National Intelligence *National Security Space Strategy, Unclassified Summary*. January 2011, 1. https://fas.org/irp/eprint/nsss.pdf.

[19] Ibid., 3.

[20] Clapper, James. "Worldwide Threat Assessment of the U.S. Intelligence Community." Statement for the Record to the Senate Armed Services Committee, February 26, 2015, 7-8.

[21] U.S. Department of Defense. *Military and Security Developments Involving the People's Republic of China 2014*. 2014, 11. http://archive.defense.gov/pubs/2014_DoD_China_Report.pdf.

[22] Ibid., 32.

[23] Clark, Colin. "U.S. Military Losing Edge in Space: Kendall." Breaking Defense, March 17, 2015. http://breakingdefense.com/2015/03/us-military-losing-edge-in-space-kendall/.

[24] Colby, Elbridge. *From Sanctuary to Battlefield*. Center for A New American Security, 2016, 9.

[25] This is the altitude of the Kármán Line, "where an aircraft would have to travel at a speed greater than orbital velocity to get enough lift from its wings to stay in the air." Theodore von Kármán co-founded the Jet Propulsion Laboratory at the California Institute of Technology and was a towering figure in the early development of U.S. rocketry and aerospace science. See "A brief history of space," Institute of Physics. http://www.iop.org/resources/topic/archive/space/index.html.

[26] *Aviation Week and Space Technology*, August 25, 2014, 19.

[27] Xu's comments reportedly appeared in the *People's Liberation Army Daily*. See "China Declares Space War Inevitable." *DOD Buzz,* November 4, 2009.

[28] Chase, Michael, Jeffrey Engstrom, Tai Ming Cheung, Kristen Gunness, Scott Warren Harold, Susan Puska, Samuel Berkowitz. "China's Incomplete Military Transformation: Assessing the Weaknesses of the People's Liberation Army (PLA)." Rand Corporation, 2015, 116. http://www.rand.org/content/dam/rand/pubs/research_reports/RR800/RR893/RAND_RR893.pdf.

[29] "Neighborhood Watch In Space." *Aviation Week and Space Technology,* August 4, 2014, 12.

[30] Ibid. Also see "Orbital MRO." *Aviation Week and Space Technology,* March 24, 2014, 29.

[31] Ibid.

[32] Shou, Xiaosong (寿晓松), ed. (*Zhanlue Xue* 战略学) [The Science of Military Strategy], 3rd ed., Beijing: Military Science Press, 2013, 178–179, 181–182, 186.

[33] Bao, Shixiu, 2007, cited at http://www.jamestown.org/programs/chinabrief/single/?tx_ttnews%5Btt_news%5D=37699#.Vy0GLEus31o.

[34] Pollpeter, Kevin, Leah Caprice, Robert Forte, Ed Francis, and Allison Peet. S*eizing the Ultimate High Ground: Chinese Military Writings on Space and Counter-Space*. Defense Group, Inc., April 2009, 12.

[35] Ibid.

[36] Pan, Youmu. (*Fei Jiechu ZhanzhengYanjiu* 非接触战争研究) [*Non-Contact Warfare Research*]. National Defense University Press, 2003, 118.

[37] Pollpeter et al. *Seizing the Ultimate High Ground*.

[38] Ibid.

[39] Santamarta, Ruben. "A Wake-up Call for SATCOM Security," IOActive, 2014. http://www.ioactive.com/pdfs/IOActive_SATCOM_Security_WhitePaper.pdf.

[40] Clapper, James. "Worldwide Threat Assessment of the US Intelligence Community," Statement for the Record to the Armed Services Committee, United States Senate, February 9, 2016, 9-10.

[41] Hu, Jintao. (*Renqing Xin Shiji Xin Jieduan Wo Jun Lishi Shiming* 认清新世纪新阶段我军历史使命) [Recognize the New Historic Missions]. December 24, 2004. http://gfjy.jxnews.com.cn/system/2010/04/16/011353408.shtml. For further discussion of the "new historic missions," see Hartnett, Daniel. *Towards a Globally Focused Chinese Military: The Historic Missions of the Chinese Armed Forces*. CNA Corporation, 2008.

[42] Mulvenon, James. "Chairman Hu and the 'New Historic Missions,'" *China Leadership Monitor* 27 (Winter 2009).

[43] Zhang, Xiaotian. "On the Development of National Interests and Development of Military Strategy." *China Military Science* 3 (2010), 7.

[44] Chang, Xianqi. *Military Astronautics*. 2nd ed. Beijing, PRC: National Defense Industries Press, 2005, 314-247.

[45] Gao, Yubiao, Chief Editor, Joint Campaign Course Materials. Beijing, PRC: Academy of Military Science Publishing House, August 2001, 54.

[46] Zhang, Yuwu, Dong Zean et al. "Informationalized Warfare Will Make Seizing the Aerospace Technology 'High Ground' a Vital Factor." *People's Liberation Army Daily,* 2005. Also see Liu, Kejian and Wang Xiubo. *The First Conflict Won Through Air-power: the Kosovo War*. Beijing, PRC: Academy of Military Science Publishing House, 2008, 44.

[47] Wang, Guanzhong, "Strive to Build Strong National Defense and Powerful Armed Forces Commensurate with China's International Standing, National Security, and Development Interests." *China Military Science* 1. (2013), 6.

[48] Chinese Military Encyclopedia Committee, *Chinese Military Encyclopedia,* Vol. II,(Beijing, PRC: Academy of Military Science Publishing House, July 1997), 126-127.

[49] Wang, Houqing, and Zhang Xingye, Eds. *The Science of Campaigns*. Beijing, PRC: National Defense University Publishing House, 2000, 88.

[50] Gao, Yubiao, ed. *Joint Campaign Course Materials*. (Beijing, PRC: Academy of Military Science Publishing House, 2001, 27.

[51] Finkelstein, David. "China's National Military Strategy: An Overview of the 'Military Strategic Guidelines." *Right-Sizing the People's Liberation Army: Exploring the Contours of China's Military*. Strategic Studies Institute, 2007, 96.

[52] Bai, Bangxi and Jiang Lijun. "Systems of Systems Conflict Is Not the Same as Systems Conflict." *National Defense Newspaper,* January 10, 2008.

[53] Ibid.

[54] Research Department, People's Liberation Army National Defense University. *China Military Encyclopedia, Strategy.* Beijing, PRC: Encyclopedia of China Publishing House, 2007, 211.

[55] Ibid.

[56] Xie, Zheng. *On Informationized Operations.* Beijing, PRC: AMS Publishing House, 2007, 154.

[57] Ibid., 154-155.

[58] Xu, Tianran, "China's Anti-Missile Test Successful: Gov't." *Global Times,* January 29, 2013. http://www.globaltimes.cn/content/758804.shtml. Also see "China Says Missile Defense System Test Successful," Associated Press, January 12, 2010. http://www.smdailyjournal.com/article_preview.php?type=wnews&id=122693.

[59] Hsu, Jeremy. "Chinese Satellites Bump During Secret Maneuvers." Space.com, September 3, 2010. http://www.space.com/missionlaunches/china-satellite-secret-orbit-maneuvers-100903.html.

[60] David, Leonard. "Mysterious Actions of Chinese Satellites Have Experts Guessing." Space.com, September 9, 2013. http://www.space.com/22707-china-satellite-activities-perplex-experts.html.

[61] Chang, Xianqi. *Military Astronautics.* 2nd ed. Beijing, PRC: National Defense Industries Press, 2005.

[62] Kan, Shirley, ed. "China-U.S. Aircraft Collision Incident of April 2001: Assessments and Policy Implications." Congressional Research Service, October 10, 2001. https://www.fas.org/sgp/crs/row/RL30946.pdf.

[63] Pan, Youmu, Non-Contact Warfare Research, Beijing, National Defense University Press, 2003, 118.

[64] Creedon, Madelyn. Assistant Secretary of Defense for Global Security Affairs. Presentation at the Stimson Center, September 13, 2013.

[65] La Vone, Michelle. "The Kessler Syndrome Explained," *Space Safety Magazine,* September 15, 2014. http://www.spacesafetymagazine.com/space-debris/kessler-syndrome.

[66] Kahn, Herman. *On Thermonuclear War,* Princeton University Press, 1960, 192.

[67] Adapted from Krepon, Michael and Julia Thompson, eds. *Anti-satellite Weapons, Deterrence and Sino-American Space Relations,* Stimson Center, October 2013. See MacDonald chapter, "Deterrence and Crisis Stability in Space and Cyberspace," 81-98.

[68] A Track 2 discussion is one in which experts and former government officials of one country meet with comparable individuals from one or more other countries. Such discussions almost always take place off of any official or public record. A Track 1 discussion is a meeting of government officials from different countries. A Track 1.5 discussion is an off-the-record discussion involving a mix of government officials, former government officials, and experts from two or more countries.

[69] In this case, "tactical" refers to purely localized use of space offense in support of a conventional operation.

[70] All views are the author's and do not reflect the opinions of the Rand Corporation or any element of the U.S. government.

[71] These terms are virtually synonymous; strong crisis stability essentially means that deterrence is unlikely to fail in a crisis.

[72] The author wishes to apologize for yielding to the temptation to deploy this cliché.

[73] The same generally can be said of the other domains, though a conflict limited to cyberspace is perhaps easier to envision than a conflict contained within another domain.

[74] This is the most basic reason why wars tend to escalate: it is rare for neither side in a conflict to stand to benefit from expanding or intensifying the fighting. See Forrest E. Morgan, Karl P. Mueller, Evan S. Medeiros, Kevin L. Pollpeter, and Roger Cliff, *Dangerous Thresholds: Managing Escalation in the 21st Century* (Santa Monica: Rand, 2008), Chapter 2.

[75] For further discussion, see Mueller, Karl P., Jasen J. Castillo, Forrest E. Morgan, Negeen Pegahi, and Brian Rosen. *Striking First: Preemptive and Preventive Attack in U.S. National Security Policy,* Rand, 2006.

[76] The "ladder of escalation" greatly overstates the predictability and discreteness of escalation thresholds, but worse, one cannot "fall up a ladder" as adversary powers may lose control in crisis escalation.

[77] U.S. Air Force. *Air Force Doctrine Document* 3-14: Space Operations.

[78] Launching effective ASAT attacks, especially in quantity, still would not necessarily be easy.

[79] SLBMs were strategically defensive in stricter terms before achieving their present high accuracy.

[80] Jervis, Robert. "Cooperation Under the Security Dilemma." *World Politics* 30:2 (January 1978).

[81] This situational dependence is not limited to space. See Glaser, Charles, and Chaim Kaufmann. "What is the Offense-Defense Balance and Can We Measure It?" *International Security* 22:4 (Spring 1998).

[82] Machiavelli, Niccolò. *The Prince,* 1532.

[83] See, for example, Pollpeter et al., *Seizing the Ultimate High Ground,* 43-44.

[84] Yang, Hua, Chen Changming, Ling Yongshun, and Ma Donghui. "Analysis of Attack and Jamming of Spaceborne Missile Advanced Early Warning System," *Aerospace Electronic Warfare,* 7 and 37. Noted in Pollpeter et al.

[85] Perry et al. *America's Strategic Posture,* 71.

[86] White House. *Fact Sheet on U.S. Space Policy*.

[87] U.S. Defense Advanced Research Projects Agency. "Airborne Launch Assist Space Access (ALASA)." http://www.darpa.mil/program/airborne-launch-assist-space-access.

[88] For example, see Rolf Anker Ims. "On the Adaptive Value of Reproductive Synchrony as a Predator-Swamping Strategy." *The American Naturalist* 136:4 (1990): 485-498. http://www.jstor.org/stable/2462190.

[89] "Sensory Input," Aviation Week and Space Technology, November 3/10, 2014, 36.

[90] Martinage, Robert. *Toward A New Offset Strategy: Exploiting U.S. Long-Term Advantages to Restore U.S. Global Power Projection Capability.* Center for Strategic and Budgetary Assessments, 2014, iv.

[91] Ibid., 56.

[92] The annual growth rate of China's GDP has already slowed from 10% to a 2015 level that China itself estimated to be under 7%.

[93] Miller, Steve. "Lighter, Stronger, More Affordable: DARPA's Quests in the Realm of Materials Science." *50 Years of Bridging the Gap,* U.S. Defense Research Projects Agency, 2008, 128.

[94] Shirer, William. *The Rise and Fall of the Third Reich,* 1960, 1085-1088.

[95] Chase, Michael et al. "China's Incomplete Military Transformation," 3.

[96] U.S. Department of Defense. "Report of Secretary of Defense Harold Brown to the Congress on the FY 1979 Budget, FY 1980 Authorization Request and FY 1979-1983 Defense Programs." January 23, 1978, 65. http://www.dod.mil/pubs/foi/logistics_material_readiness/acq_bud_fin/247.pdf.

[97] MacDonald, Bruce et al. *Anti-satellite Weapons, Deterrence and Sino-American Space Relations.*

[98] U.S. Department of Defense. "Fact Sheet: Resilience of Space Capabilities," 2011. http://archive.defense.gov/home/features/2011/0111_nsss/docs/DoD%20Fact%20Sheet%20-%20Resilience.pdf.

[99] Gruss, Mike. "GAO: U.S. Air Force Needs More Info Before Committing to Disaggregation." *Space News,* November 5, 2014. http://spacenews.com/42464gao-us-air-force-needs-more-info-before-committing-to-disaggregation/.

100 U.S. Air Force Space Command. "Resiliency and Disaggregated Space Architectures." 2013, 3. http://www.afspc.af.mil/shared/media/document/AFD-130821-034.pdf.

101 U.S. Department of Defense. "Fact Sheet: Resilience of Space Capabilities."

102 Ibid.

103 U.S. Government Accountability Office. "DOD Space Systems: Additional Knowledge Would Better Support Decisions about Disaggregating Large Satellites." October 30, 2014. http://gao.gov/assets/670/666716.pdf.

104 "DHS Cyber Chief Emphasizes Resiliency, Building Trust." *Federal Times,* September 26, 2014.

105 U.S. Government Accountability Office. "DOD Space Systems."

106 U.S. Department of Defense. "Fact Sheet: Resilience of Space Capabilities."

107 Martinage, Robert. *Toward A New Offset Strategy: Exploiting U.S. Long-Term Advantages To Restore U.S. Global Power Projection Capability,* Center for Strategic and Budgetary Assessments 2014, 49.

108 The report was delivered to the Secretary General in July 2013 and approved by the UN General Assembly that autumn. For a longer discussion of this draft, see Gandenberger, Mia. "Russia and China table new draft treaty to prevent weapons in space." Reaching Critical Will, 2014, 90. http://www.reachingcriticalwill.org/disarmament-fora/cd/2014/cd-reports/8908-russia-and-china-table-new-draft-treaty-to-prevent-weapons-in-space.

109 For a longer discussion of the GGE, see Johnson, Christopher. "The UN Group of Governmental Experts on Space TCBMs." *Secure World Foundation,* 2014. http://swfound.org/media/109311/swf_gge_on_space_tcbms_fact_sheet_april_2014.pdf.

110 For a longer discussion of the CoC, see Johnson, Christopher. "Draft International Code of Conduct for Outer Space Activities Fact Sheet." Secure World Foundation, 2014. http://swfound.org/media/166384/SWF_Draft_International_Code_of_Conduct_for_Outer_Space_Activities_Fact_Sheet_February_2014.pdf.

111 For a longer discussion about a national space policy's potential role as a transparency and confidence-building measure, see Samson, Victoria. "National Space Policies and Their Importance in Ensuring the Long-Term Sustainable Use of Space." Paper presented at the 65th International Astronautical Congress, Toronto, Canada, September 29 to October 3, 2014. http://swfound.org/media/177299/iac-2014-e3_4_4_victoria_samson.pdf.

112 In unofficial dialogues between U.S. and Chinese security experts, the Chinese have expressed appreciation to their U.S. counterparts, including this report's author, for making this information available to them, as well as warnings about possible collisions between Chinese satellites and space debris.

113 As of publication, China has not followed up on its pledge to participate in a government-to-government cyber-security dialogue.

114 Pointing, Navigation, Tracking satellites (e.g., GPS, Beidou, GLONASS, Galileo)

115 "NRO Confirms Chinese Laser Test Illuminated U.S. Spacecraft." Space News, October 3, 2006. http://spacenews.com/nro-confirms-chinese-laser-test-illuminated-us-spacecraft/.

116 Also see Medeiros, Evan. "'Minding the Gap': Addressing the Trajectory of the PLA's Second Artillery." In *Right Sizing the People's Liberation Army,* edited by Roy Kamphausen and Andrew Scobell (Carlisle, PA: Strategic Studies Institute, 2007), 143-189. http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB784.pdf.

117 Colby, Elbridge. *From Sanctuary to Battlefield,* 28-29.

118 U.S. Air Force. *Exhibit R-2, RDT&E Budget Item Justification: PB 2013 Air Force.* February 2012. http://www.globalsecurity.org/military/library/budget/fy2013/usaf-peds/0604421f.pdf. The budget explanation of CSCS reads:

"This effort supports concept exploration and follow-on system development of mobile/transportable counter satellite communications capabilities derived from technologies prototyped in PE0603438F, Space Control Technology, in the area of Offensive Counter-Space. Future advanced counter satellite communications systems will also be developed in this program. Included are: architecture engineering, system hardware design and development, software design and integration, testing and procurement of capabilities to provide disruption of satellite communications signals in response to USSTRATCOM requirements."

Any official acknowledgment of an offensive counter-space capability would require careful strategic messaging to achieve the desired level of public understanding.

ABOUT THE AUTHORS

Bruce W. MacDonald is an independent consultant providing technology and policy management services and is president of Provectus Analytics, where he leads studies on China and Crisis Stability in Space; Cross Domain Dynamics; Multi-Polar Missile Defense Dynamics; and teaches at the Johns Hopkins School of Advanced International Studies. He has participated in numerous Track 1.5 and Track 2 dialogues with Chinese and other country experts addressing nuclear weapons, space/cyber conflict, missile defense, and crisis management. He directed the Federation of American Scientists' study on the security implications of Chinese missile defense developments for the United States and was Senior Director to the 2008-09 Congressional Commission on the Strategic Posture of the United States, a bipartisan body headed by former Defense Secretaries William Perry and James Schlesinger and was project leader and final report author for the Council on Foreign Relations' study of China, Space Weapons, and U.S. Security in 2007-2008.

MacDonald was Assistant Director for National Security at the White House Office of Science and Technology Policy from 1995-1999 and also served as Senior Director for Science and Technology on the National Security Council staff. He was a professional staff member of the House Armed Services Committee for Air Force acquisition, space, and BMD issues and was national security adviser to Sen. Dale Bumpers. MacDonald was a State Department specialist on nuclear weapons, space, and technology where he chaired the Inter-agency START Policy Working Group, served on the U.S. START delegation in Geneva, and worked on space, nuclear, and missile defense issues. He began his career at a defense contractor on advanced BMD concepts and strategic forces.

MacDonald graduated with honors in aerospace engineering from Princeton University and also received two masters' degrees from Princeton, one in aerospace engineering/rocket propulsion and the other in public and international affairs at the Woodrow Wilson School. He is a member of the Council on Foreign Relations and the American Institute of Aeronautics and Astronautics.

Dennis Blair is CEO and Chairman of the Board of Sasakawa Peace Foundation, USA, a think tank devoted to US-Japan relations. He serves as a member of the Energy Security Leadership Council; on the boards of Freedom House, the National Bureau of Asian Research, the National Committee on US-China Relations and the Atlantic Council. From January 2009 to May 2010, as Director of National Intelligence, Blair led sixteen national intelligence agencies, administering a budget of $50 billion and providing integrated intelligence support to the President, Congress and operations in the field. From 2003 to 2006, Blair was president and chief executive officer of the Institute for Defense Analyses (IDA), a federally funded research and development center based in Alexandria, Virginia that supports the Department of Defense, the Department of Homeland Security and the Intelligence Community. Prior to retiring from the Navy in 2002, Admiral Blair served as Commander in Chief, U.S. Pacific Command, the largest of the combatant commands. During his thirty-four-year Navy career, Admiral Blair served on guided missile destroyers in both the Atlantic and Pacific fleets and commanded the Kitty Hawk Battle Group. Ashore, he served as Director of the Joint Staff and held budget and policy positions on the National Security Council and several major Navy staffs.

A graduate of the U.S. Naval Academy, Admiral Blair earned a master's degree in history and languages from Oxford University as a Rhodes scholar, and was a White House fellow at the Department of Housing and Urban Development. He has been awarded four Defense Distinguished Service medals, three National Intelligence Distinguished Service medals, and has received decorations from the governments of Japan, Thailand, Korea, Australia, the Philippines, and Taiwan.

Blair co-chaired two commissions that issued reports on pressing national problems: The Report of the Commission on the Theft of American Intellectual Property, published in May, 2013 and Oil Security 2025: US National Security in an Era of Oil Abundance, published in January, 2014. His latest book is Military Engagement: Influencing Armed Forces Worldwide to Support Democratic Transitions, published in June, 2013.

Dean Cheng is The Heritage Foundation's senior research fellow on Chinese political and security affairs. He specializes in China's military and foreign policy, in particular its relationship with the rest of Asia and with the United States. He has written extensively on China's military doctrine, technological implications of its space program and "dual use" issues associated with the communist nation's industrial and scientific infrastructure. Previously he worked for the China Studies division of the Center for Naval Analyses, the federally funded research institute and Science Applications International Corporation (SAIC), the Fortune 500 consulting firm. Before entering the private sector, Cheng studied China's defense-industrial complex for a congressional agency, the Office of Technology Assessment, as an analyst in the International Security and Space Program.

Cheng has testified before Congress, appeared on public affairs shows such as John McLaughlin's One on One and programs on National Public Radio, CNN, BBC World Service, and International Television News (ITN). He has been interviewed by or provided commentary for publications such as Time magazine, The Washington Post, Financial Times, Bloomberg News, Jane's Defense Weekly, South Korea's Chosun Ilbo and Hong Kong's South China Morning Post, and he is the author of the forthcoming Cyber Dragon: Inside China's Information Warfare and Cyber Operations (Praeger Publishers). Cheng has spoken at the National Space Symposium, National Defense University, the Air Force Academy, Massachusetts Institute of Technology (MIT), and the Eisenhower Center for Space and Defense Studies.

Cheng earned a bachelor's degree in politics from Princeton University in 1986 and studied for a doctorate at MIT.

Karl P. Mueller is a senior political scientist at the Rand Corporation. He specializes in research related to military and national security strategy, particularly coercion and deterrence. Mueller has written and lectured on a wide variety of national security subjects, including air-power theory, grand strategy, economic sanctions, nuclear proliferation, counter-terrorism policy, space weapons, and war gaming. His recent Rand publications include Precision and Purpose: Air-power in the Libyan Civil War (2015), Denying Flight: Strategic Options for Employing No-Fly Zones (2013), Dangerous Thresholds: Managing Escalation in the 21st Century (Forrest E. Morgan et al., 2008), and Striking First: Preemptive and Preventive Attack in U.S. National Security Policy (2006). He is currently working on projects about defending the Baltic States, managing crisis escalation, and the future of U.S. air-power. Before joining Rand in 2001, Mueller was a professor of comparative military studies at the U.S. Air Force's School of Advanced Air and Space Studies (SAASS). He is currently an adjunct professor at Johns Hopkins University and in the Security Studies Program at Georgetown University. Mueller received his Ph.D. in politics from Princeton University.

Victoria Samson is the Washington Office Director for the Secure World Foundation and has more than eighteen years of experience in military space and security issues.

Before joining SWF, Samson served as a Senior Analyst for the Center for Defense Information (CDI), where she leveraged her expertise in missile defense, nuclear reductions, and space security issues to conduct in-depth analysis and media commentary. Prior to her time at CDI, Samson was the Senior Policy Associate at the Coalition to Reduce Nuclear Dangers, a consortium of arms control groups in the Washington, D.C. area, where she worked with Congressional staffers, members of the media, embassy officials, citizens, and think-tanks on issues surrounding dealing with national missile defense and nuclear weapons reductions. Before that, she was a researcher at Riverside Research Institute, where she worked on war-gaming scenarios for the Missile Defense Agency's Directorate of Intelligence. Samson is often interviewed by multinational media outlets, including the New York Times, Space News, and NPR. She is also a prolific author of numerous op-eds, analytical pieces, journal articles, and updates on missile defense and space security matters. Samson holds a Bachelor of Arts (B.A.) degree in political science with a specialization in international relations from UCLA and a Master of Arts (M.A.) in international relations from the Johns Hopkins School of Advanced International Studies.

The Foreign Policy Institute
The Paul H. Nitze School of
Advanced International Studies
Johns Hopkins University
Rome Building, Suite 734
1619 Massachusetts Avenue, N.W.
Washington, D.C. 20036
Tel: +1 202 663 5772
www.fpi.sais-jhu.edu
@FPI_SAIS

The Foreign Policy Institute (FPI) of The Johns Hopkins University's Paul H. Nitze School of Advanced International Studies (SAIS) was established in 1980 to unite the worlds of scholarship and policy in the search for realistic solutions to critical international challenges. The FPI is committed to advancing global agendas by providing a neutral forum for discussion, debate and dialogue and serving as a source of rigorous analysis and relevant policy ideas addressing the foreign policy and international security challenges of our time.

FPI STUDIES IN POLICY

For more than three decades, leading experts and scholars have addressed critical topics in foreign policy and security through the publication of independent, policy relevant analyses through the FPI. The FPI is proud to build on this tradition with the FPI Studies in Policy series, featuring monograph-length studies of politics, economics, and political economy that inform current international policy and security debates.