MARCH 2020

ON THE RADAR

UNDER THE NUCLEAR SHADOW

Situational Awareness Technology and Crisis Decisionmaking

AUTHORS

Rebecca Hersman
Reja Younis
Bryce Farabaugh
Bethany Goldblum
Andrew Reddie

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

MARCH 2020

ON THE RADAR

UNDER THE **NUCLEAR SHADOW**

Situational Awareness Technology and Crisis Decisionmaking

AUTHORS

Rebecca Hersman
Reja Younis
Bryce Farabaugh
Bethany Goldblum
Andrew Reddie

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

About CSIS

The Center for Strategic and International Studies (CSIS) is a bipartisan, nonprofit policy research organization dedicated to advancing practical ideas to address the world's greatest challenges.

Thomas J. Pritzker was named chairman of the CSIS Board of Trustees in 2015, succeeding former U.S. Senator Sam Nunn (D-GA). Founded in 1962, CSIS is led by John J. Hamre, who has served as president and chief executive officer since 2000.

CSIS's purpose is to define the future of national security. We are guided by a distinct set of values—nonpartisanship, independent thought, innovative thinking, cross-disciplinary scholarship, integrity and professionalism, and talent development. CSIS's values work in concert toward the goal of making real-world impact.

CSIS scholars bring their policy expertise, judgment, and robust networks to their research, analysis, and recommendations. We organize conferences, publish, lecture, and make media appearances that aim to increase the knowledge, awareness, and salience of policy issues with relevant stakeholders and the interested public.

CSIS has impact when our research helps to inform the decisionmaking of key policymakers and the thinking of key influencers. We work toward a vision of a safer and more prosperous world.

CSIS is ranked the number one think tank in the United States by the University of Pennsylvania's annual think tank report.

CSIS does not take specific policy positions; accordingly, all views expressed herein should be understood to be solely those of the author(s).

ISBN: 978-1-4422-8153-0 (pb); 978-1-4422-8154-7 (ebook)

Center for Strategic & International Studies
1616 Rhode Island Avenue, NW
Washington, D.C. 20036
202-887-0200 | www.csis.org

Rowman & Littlefield
4501 Forbes Boulevard
Lanham, MD 20706
301-459-3366 | www.rowman.com

Acknowledgments

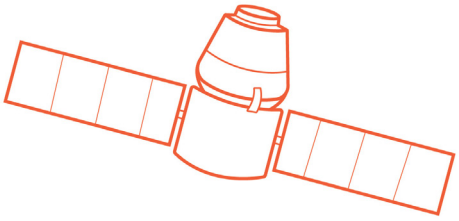
This report is the culmination of a two-year study by CSIS' Project on Nuclear Issues (PONI) and the Nuclear Policy Working Group (NPWG) at the University of California, Berkeley, on the emerging strategic situational awareness (SA) environment and its impact on nuclear crises. The research team hopes that this report's findings and analysis can inform the U.S. policy, military, and technical communities to better equip decisionmakers for crises.

We want to express our deepest gratitude to Bernadette Stadler for her research work and management of this project from its outset and wish her the best in her graduate studies. A special thank you to those who researched for this project along the way: Alex Lenser, Lizamaria Arias, and Shannon Kearney. We would like to thank our consultants—Kate Charlet, Jared Dunnmon, Michael Horowitz, Elsa Kania, Philip Reiner, Jason Arterburn, and Paul Scharre—each of whom went above and beyond to help us understand key aspects of this complex issue set.

We relied on the expertise of many other CSIS colleagues, including Eric Brewer, Maxwell Simon, Rhys McCormick, Kaitlyn Johnson, and Lindsey Sheppard, for their research insights. Rebecka Shirazi and Jeeah Lee did an outstanding job managing the publication process. We are thankful to have collaborated with the creative members of the Andreas C. Dracopoulos iDeas Lab: Emily Tiemeyer for graphic design; Jacqueline Schrag and Tucker Harris for construction and design of our microsite; and Mark Donaldson and Christopher Burns for producing videos used in our tabletop exercises. Over 150 next-generation scholars, mid-career professionals, and senior experts participated in our tabletop exercises, providing insights which shaped this study's research findings and recommendations. Both CSIS PONI Nuclear Scholars and members of the NPWG contributed extensively to the writing of technology and country primers on the website.

The authors alone are responsible for the report's findings and recommendations and any errors in fact, analysis, or omission. This report is made possible by support from the Carnegie Corporation of New York.

Contents



1 | Introduction

For most of the nuclear age, enhanced strategic situational awareness (SA)—the ability to characterize the operating environment, detect nuclear and conventional strategic attacks, and discern real attacks from false alarms—has been viewed as a benefit to crisis stability as well as a relatively free good that can be obtained with limited risk. By improving the accuracy and timeliness of warning, increasing visibility and clarity on adversary actions, and extending decision time in crisis, improved SA reduced the risk of miscalculation at the nuclear level and use-or-lose pressures that could incentivize a nuclear first strike. Moreover, the systems that provided this strategic warning operated at long range, from outside of adversary territories, and generally in ways that were not visible or particularly concerning to an adversary because they offered little in terms of first-strike advantage.[1]

In conventional conflicts with non-nuclear adversaries, the United States has long enjoyed information dominance and suffered few repercussions for the asymmetric advantage it has offered. Information dominance has been essential to ensuring U.S. military effectiveness, sustaining the credibility and assurance of military alliances, and stabilizing or reducing the risks of miscalculation or collateral damage.[2] But can there be too much of a good thing? As the strategic SA ecosystem evolves, it seems ever more possible that actions taken to improve strategic SA may increase the risk of escalation and upset crisis stability. Conversely, concerns about escalation may cause reluctance among decisionmakers to use capabilities that could better illuminate a crisis and reduce the risk of war.

Three geostrategic trends challenge the inherent stabilizing value of information dominance in crises and conflicts.

First, in today's increasingly competitive and complex security environment, the risk of crisis or conflict between nuclear-armed states is on the rise.[3] Russia's growing militarism along NATO's periphery raises concerns about the potential for a serious crisis between the world's largest nuclear powers, and China's increasingly-assertive territorial claims in the South China Sea pose challenges to U.S. interests in the Pacific.[4] At the same time, rising regional tensions and growing nuclear capabilities of previously second- or third-tier nuclear-armed states add risk and complexity to escalatory dynamics.[5] A lack of clear thresholds and triggers for

Information dominance has been essential to ensuring U.S. military effectiveness, sustaining the credibility and assurance of military alliances, and stabilizing or reducing the risks of miscalculation or collateral damage. But can there be too much of a good thing?

possible conflict in this increasingly multipolar environment may play out in novel and unprecedented ways, including through the capabilities and concepts that undergird future strategic SA.

Second, the capabilities designed to provide SA and support senior decisionmakers in crises and conflicts are increasingly comingled into a single conventional/nuclear ecosystem. Convenience, reduced costs, and flexibility are motivating decisionmakers to increasingly rely on strategic tools such as early-warning and communications systems for conventional operations—tools traditionally reserved for nuclear command and control. While attacks on, or intrusive surveillance of, these assets was considered highly escalatory and off-limits during conventional conflicts of the past, their dual-use nature today means adversaries may have difficulty discerning U.S. intent during a crisis. This comingling could increasingly force decisionmakers to weigh the benefits of rapid, decisive military victory afforded by information dominance against the high-stakes risks of nuclear escalation.

Third, some of these emerging technologies will likely provide insights into adversary actions and activities which could have unintended consequences for strategic decisionmaking. The combination of new enabling capabilities such as advanced sensor technologies, platforms for their deployment, high-bandwidth networks, and artificial intelligence (AI) tools are transforming the potential field of view at the conventional and nuclear levels of conflict. While decisionmakers have long grappled with the challenges of digesting information quickly in a crisis and detecting adversary denial and deception tactics, new SA technologies stand to compound these problems. The speed and precision of these capabilities will likely increase decisionmakers' knowledge of adversary forces, deployments, and actions sooner than was previously possible, but some of this information may be vulnerable to intentional disinformation and other gray zone activity.[6] The increased amount of information itself poses another challenge insofar as processing and deriving useful knowledge from the raw data can be overwhelming for analysts.[7]

These three trends require new perspectives on the value and risks associated with information dominance in the emerging SA ecosystem and its impact on nuclear crises.

The Growing Nuclear Shadow

The nuclear dimension will overshadow any future crises or conflicts between nuclear-armed states—and bring with it the risk of escalation. Russia, China, North Korea, India, and Pakistan are all expanding their nuclear weapons capabilities and means of delivery.[8] The demise of key arms control treaties such as the Intermediate-Range Nuclear Forces Treaty, at a minimum, will make it easier for countries to develop and deploy new conventional and nuclear systems. At the same time, heightened competition between nuclear-armed states is creating complex multipolar stability dynamics. These are particularly pronounced in the Indo-Pacific region, where five nuclear-armed states—the United States, China, India, Pakistan, and North Korea—seek to achieve their security objectives in hotly contested environments and amid regional tensions.[9] As strategic competition intensifies, so too does the risk of conventional crisis or conflict.

The nuclear dimension will overshadow any future crises or conflicts between nuclear-armed states—and bring with it the risk of escalation.

And yet, the conditions necessary for strategic stability, particularly in crisis or conflict, seem poorly understood between nuclear-armed states. In an environment where a greater number of capabilities

support both conventional and nuclear missions, red lines can be miscalculated and crises difficult to control. The stakes associated with escalation between nuclear-armed states—the nuclear shadow—will always loom large, even in a conventional crisis.[10]

The Evolving Strategic Situational Awareness (SA) Ecosystem

THE TRADITIONAL STRATEGIC SA ECOSYSTEM (APPROXIMATELY 1950-1990)

The traditional strategic SA environment featured stratified and largely isolated capabilities, enabling nuclear and conventional strategic SA to operate independently.[11] The passive nature of the ecosystem was designed to detect attacks, not anticipate or disrupt them. In this bifurcated ecosystem, the bright line between strategic SA systems used for conventional and nuclear missions meant strategic SA assets could be secure and compartmentalized.

The traditional strategic SA environment emerged during the Cold War and focused on understanding a near-peer adversary's nuclear forces and warning of nuclear attack. It consisted primarily of early-warning radars, satellites, hydroacoustic stations, and seismometers located around the world.[12] These passive systems were viewed as stabilizing in part because they were designed to detect attacks, not predict them. Furthermore, these technologies were stratified. They were focused almost exclusively on collecting information on nuclear systems. The bright line between systems used for nuclear and conventional SA reduced the possibility of inadvertent escalation by reinforcing the perceived "firebreaks" between conventional and nuclear conflict. Moreover, since strategic SA assets were secure and compartmentalized (operating from space or remote locations), these systems were difficult to target kinetically. Other parts of the system, such as command and control (C2), contained substantial redundancies and were considered invulnerable to attack.

The secure and compartmentalized nature of the traditional SA environment generally yielded high confidence in information these systems provided, limited their vulnerability to attack and

The Aurora Borealis lights are visible over Thule Air Base, Greenland Dec 11, 2017. Thule is the most northern base United States military members are stationed at around the world, and is charged with the mission of missile warning, space surveillance and satellite command and control.

U.S. Air Force photo by Senior Airman Dennis Hoffman

manipulation, and reduced the chances of miscalculation. As a result, these systems came to be viewed as contributing positively to strategic stability by ensuring confidence in the durability of the overall nuclear deterrent and reducing risks of premature or miscalculated nuclear use. In this environment, policymakers had long assumed that adversaries would be deterred from attacking satellites involved in nuclear command, control, and communications (NC3).

THE TRANSITIONAL STRATEGIC SA ECOSYSTEM (APPROXIMATELY 1990-2020)

In the transitional strategic SA ecosystem, technological innovation and development drove enhancements to the conventional SA ecosystem which in turn afforded the United States unequaled information dominance and enabled the emergence of precision warfare. At the same time, nuclear SA assets became more important to supporting conventional missions, especially in the areas of NC3. While still possessing somewhat distinct elements, the two ecosystems became increasingly less compartmentalized. Over this period, a wider range of state actors and commercial entities developed advanced information gathering and communications technology, such as remote sensing satellite capabilities.[13]

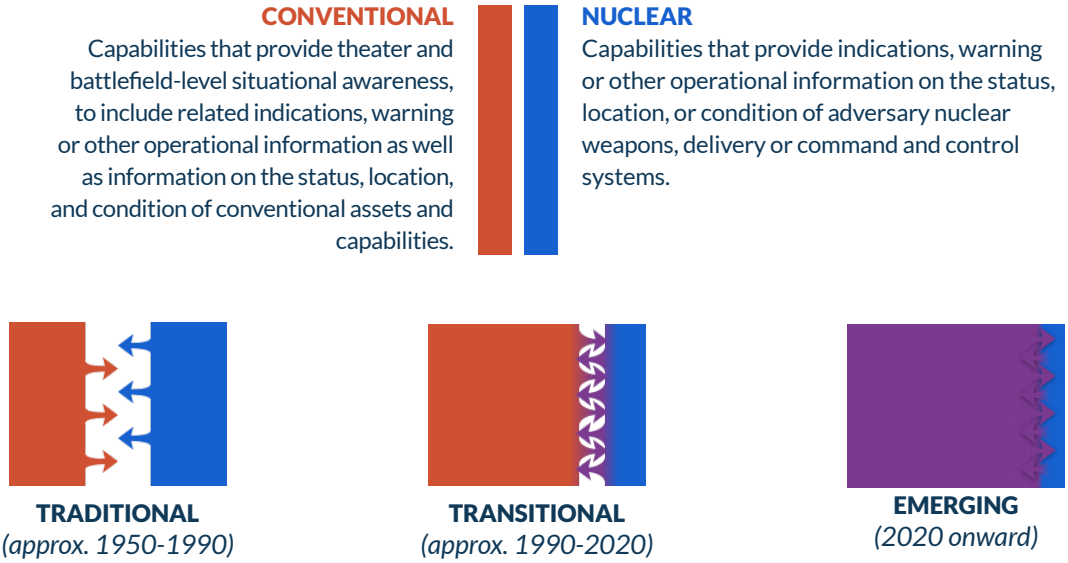
Indeed, the origin of the transitional strategic SA environment can be traced back to the 1990s. Technological developments throughout the second half of the twentieth century culminated in the networked battlefield of the Gulf War. The Gulf War saw the employment of effective communications, command, control, and intelligence (C3I), which gave commanders dramatically improved SA by making use of strategic systems for conventional purposes, especially in terms of precision targeting. Counterterrorism efforts, from Afghanistan to Iraq and al-Qaeda to the Islamic State of Iraq and the Levant (ISIL), relied heavily on these advancing strategic SA capabilities—from satellite-hosted sensors to advanced drone technology—to provide actionable information in areas where U.S. freedom of action was fairly high and the strategic stability implications quite low.

Critically, whereas the traditional strategic SA environment contained systems that were either focused on nuclear warning ("nuclear" strategic SA systems) or on providing intelligence to commanders about the conventional battlefield ("conventional" strategic SA), in the transitional strategic SA environment, dual-use strategic SA capabilities were increasingly tasked to conduct both missions. The United States stopped using various nuclear-only communications assets, including the Emergency Rocket Communications System and the Survivable Low Frequency Communication System. Advanced Extremely High Frequency (AEHF) and MILSTAR satellites began to provide communications support for nuclear and nonnuclear missions.[14] In this environment, the compartmentalization of nuclear and conventional SA systems and the stabilizing nature of transparency at the nuclear level became less well defined. Indeed, with the exception of nuclear weapon delivery system control capabilities, each of the assets associated with the NC3 system mentioned by the 2018 Nuclear Posture Review is dual use.[15]

THE EMERGING STRATEGIC SA ENVIRONMENT (2020 FORWARD)

The emerging strategic SA ecosystem is highly networked, operates in real-time, and is dual use, creating a landscape that is highly capable but also murkier and more complex. Figure 1.1 demonstrates the three stages of the evolution of the SA ecosystem—traditional, transitional, and emerging. In the emerging SA environment, not only do conventional weapons rely on strategic SA assets for targeting data, countries will also rely on conventional SA systems for strategic warning. For example, hypersonic weapons, boost-glide systems, long-range cruise missiles, and other capabilities are designed to elude traditional U.S. early-warning systems (e.g., radars and

Figure 1.1



satellites), reduce confidence in strategic warning, and defeat U.S. missile defenses. To counter these new delivery systems, the United States may have to rely on conventional SA systems, including systems that are more visible or intrusive, to provide nuclear warning, support nuclear missions, and supplement strategic SA. If an adversary were to discover and target such surveillance systems, would such an attack be considered conventional or strategic in intent and implication?

The emerging strategic SA ecosystem is highly networked, operates in real-time, and is dual use, creating a landscape that is highly capable but also murkier and more complex.

Increasingly blurred lines in NC3 also contribute to this dynamic. For example, conventional missile warning currently relies on these dual-use surveillance capabilities, increasing the risk that they could be targeted in a conventional conflict for conventional purposes but with profound strategic implications. The rapid pace of technological advancement, the dual-use (nuclear and conventional) applicability of emerging capabilities, and the blurring of lines within NC3 are reshaping the emerging landscape. This new SA ecosystem can provide vast amounts of information more quickly and more precisely than ever before, including on strategic threats that may prove elusive to traditional warning systems. That said, given the high stakes involved in a conflict between nuclear-armed states, adversaries may be far less likely to allow such information dominance to proceed unchecked.

This emerging ecosystem is marked by a number of paradoxes. Advances in remote sensing technologies can provide policymakers unprecedented levels of visibility into adversary capabilities, yet its collection will require major advances in data analysis and decision-support systems to process and translate vast amounts of data. Improving AI and vehicle technologies such as robotics and autonomy will enable autonomous collection platforms that expand access and reduce operational risks associated with manned surveillance while lowering the stakes for adversaries to destroy or

Figure 1.2

disable surveillance and warning assets. Reducing barriers between conventional and nuclear forces may enhance crisis management in complex nuclear scenarios, but this comingling could increase misperceptions about intentions and nuclear risks.

Pathways to Escalation

The technological capabilities in the emerging strategic SA environment have the potential to dramatically improve decisionmakers' understandings of developing conflicts and improve crisis management and response. However, it is possible that the use of these capabilities may complicate crisis management and introduce new or underappreciated escalatory risks. Of particular concern are three potential escalation pathways—provocation, entanglement, and information complexity—that may be triggered or exacerbated by the use of emerging strategic SA-enhancing capabilities.

PROVOCATION

Escalation through provocation can occur when parties to a crisis perceive information collection activities as offensive in nature or believe such actions create an offensive advantage. On this pathway, one or both parties may believe escalatory steps are controllable or unavoidable. This inability to delineate intentions can result in a spiraling sequence of tit-for-tat actions and reactions and a loss of escalatory control. The active nature of the emerging strategic SA ecosystem means that states have the capability to penetrate adversary territory (via land, sea, and air) and networks, with the potential to gain highly precise and potentially actionable information. However, these capabilities directly challenge legal and political concepts of sovereignty, their mission (general surveillance versus counterforce support or surveillance versus strike) may not always be readily identifiable, and they may intentionally or unintentionally approach vital strategic assets as they conduct surveillance.

In addition, the applicability of these strategic SA capabilities to inform or enable preventive or preemptive action further complicates these offense/defense perceptions and may introduce highly provocative first-mover incentives. As strategic SA capabilities improve, the counterforce value associated with advanced surveillance capabilities will grow as well. The increasing precision of information gathering assets—such as more diverse sensor platforms, advanced sensor technology, and increased data transmission speeds—is making it more challenging to effectively conceal one's nuclear arsenal and delivery systems.[16] In such cases, the actual or perceived ability of technologically advanced countries to carry out precision-strike missions against strategic nuclear assets could make any SA-enhancing activities, even those purely defensive in nature, seem provocative or escalatory. For example, if North Korea suspected that the United

States had the capability to track and destroy North Korean nuclear mobile missiles, it might assume that any U.S. intelligence, surveillance, and reconnaissance assets in North Korean airspace were a threat to its nuclear assets regardless of the actual assigned mission. In this situation, North Korea may be motivated to launch nuclear weapons before its nuclear-armed systems could be disabled.[17]

ENTANGLEMENT

Escalation through strategic SA entanglement happens when parties to a crisis or conflict are unable to delineate between nuclear and conventional risks. The blending of conventional and nuclear strategic SA capabilities in a single ecosystem may increase the risk of miscalculation and unintended escalation. Factors like the increasing vulnerability of or reliance on dual-use C3I assets increases risks associated with misinterpreted warning, closing the damage-limitation window, and crisis instability.[18] These risks can lead decisionmakers to believe either that their own nuclear forces are vulnerable to a disarming strike or that there is an opportunity to disarm an adversary. More specifically, entanglement in the strategic SA space occurs when conventional SA systems intentionally or unintentionally collect information on nuclear assets or when dual-use SA systems become military targets during a conventional conflict. These risks are especially pronounced in crisis situations, as threats to dual-use assets used for strategic warning, communications, or command and control can be perceived as actions meant to "blind" an adversary in preparation for a nuclear strike. Actions meant solely to collect information (either conventional or nuclear) can be viewed as escalatory under these circumstances if decisionmakers believe there is a chance the crisis may escalate to nuclear conflict.

INFORMATION COMPLEXITY

...information complexity results from decisionmakers' inability to seek, manage, and interpret information effectively.

Both the quantity and quality of information generated by the emerging strategic SA ecosystem have the potential to contribute to escalation in surprising ways. Escalation through information complexity results from decisionmakers' inability to seek, manage, and interpret information effectively. This can result in decisional paralysis or biased decisionmaking, which in turn can impair effective crisis management. In the national security field, it is widely assumed that more and better information, provided more quickly, leads to more decision time and therefore better decisionmaking. However, this may not always be the case. In a complex information environment where data may be neither easily understood nor highly trusted and relies on unfamiliar technologies, cognitive processes could increase both the risks and the stakes in crisis decisionmaking.[19] The technologies in the emerging strategic SA ecosystem have the potential to provide vast amounts of information; however, this information must be analyzed and distilled in a way that is useful.[20] It must inspire confidence rather than mistrust.[21] The ambiguous and unproven nature of some of the new streams of strategic SA may lead decisionmakers to discount vital information if they do not trust the source.[22] Moreover, while excessive caution may avoid unnecessary provocation, it may also force decisionmakers and military operators to "fly blind" in a crisis in ways that contribute to miscalculation, either resulting in escalation or de-escalation on highly unfavorable terms. This suggests that psychology, particularly in the form of pre-held beliefs and cognitive biases, is underappreciated when examining the relationship between crisis decisionmaking and emerging technology. New technologies should be socialized with policymakers well before the onset of a crisis to improve the likelihood that policymakers will trust and use them appropriately.

Evolution or Revolution?

Technology promises to change the way collectors, analysts, and decisionmakers use information going forward in the emerging strategic SA environment, but not all technologies are created equal. With that in mind, there is room for discussion about: (1) whether these capabilities should be viewed as iterative improvements that do not fundamentally refashion the strategic SA landscape and the challenges decisionmakers will face (the "evolution" perspective); or (2) whether they represent such significant advancements that they will significantly transform conflict management in the years to come (the "revolution" perspective).

The "On the Radar" project took an expansive look at emerging technologies, drawing examples from across all domains (land, sea, air, space, and cyber), all levels of development (from early stage to already in the field), and all levels of utility. The research team relied exclusively on unclassified, publicly available sources to assess these capabilities, and certain capabilities may be more advanced than open sources indicate. While it is unclear whether ongoing technological advancements in strategic SA should be classified as either "evolution" or "revolution" (given the historic hindsight required for such an assessment), what is clear today is that the emerging environment is functionally different—the combination of technologies, when taken together, are likely to create an ecosystem of substantially increased information, with implications across the spectrum of conflict.

Some technologies may be more "revolutionary" than others. For example, some have predicted that computer hardware and software, AI, and robotics may undergo the most transformative changes over the 2020 to 2040 period in comparison to other military technologies.[23] These technologies are integral in many strategic SA capabilities; unmanned vehicles, autonomous platform control, and cyber surveillance all rely heavily on advances made in these areas, which may impact their continued relevance in the ecosystem moving forward.

Technologies can be prone to intermittent development, however, which strengthens the "evolution" perspective. For example, while Moore's Law has traditionally predicted that the number of components on an integrated circuit would double approximately every two years, chip designers have started running into problems working at the seven nanometer-scale, which could have implications for the miniaturization trend that has fueled advances in such disparate strategic SA technologies as unmanned aerial vehicles (UAVs) to sensors.[24] Additionally, while AI technologies have made significant advances in the past 10 years, some experts fear an approaching "AI winter," wherein AI development slows significantly in response to technical or financial barriers.[25]

While the "evolution" versus "revolution" debate will surely continue as strategic SA technologies develop and are combined in new and unforeseen ways, taking a holistic view of the myriad technologies can help illustrate potential ways the ecosystem could develop.

The Path Forward

The transformational nature of the strategic SA landscape suggests a re-examination is necessary to consider the risks these emerging capabilities may introduce, as well as the challenges they may pose for policy professionals, especially when employed in a crisis or conflict between nuclear-armed states. Finding a balance between costs and benefits in such a complex security environment, while also maximizing the value of information in terms of terminating a crisis or conflict on favorable terms, will not be easy. Tactical or operational collection decisions—such as where unmanned aircraft can fly or which cyber systems will be penetrated—will be infused with strategic meanings and consequences. Surveillance

capabilities will be expected to perform roles beyond gathering information, to include signaling resolve, reassurance, or restraint. Against a non-nuclear adversary, the discovery, loss, or misuse of a capability may confuse or provoke but is unlikely to risk a nuclear war. Against a nuclear adversary, the risks and the potential consequences, are quite different.

Moving forward, the networked and dual-capable nature of many conventional systems may force a different approach to escalation management that places less reliance on traditional conventional/nuclear firebreaks. The emerging SA ecosystem can create new risks but also ameliorate them depending on how these capabilities are used and communicated. To effectively manage crisis escalation, decisionmakers must understand how the strategic SA ecosystem has evolved, appreciate the dynamic relationship between improved strategic SA and crisis stability, and recognize the complex interplay between technology, escalation, and decisionmaking.

REPORT ROADMAP

This report proceeds as follows: Chapter 2 is an analysis of the emerging SA ecosystem, the attributes of relevant technologies, and a global look at select countries and their current SA capabilities. Chapter 3 is an overview of the risk factors that may undermine strategic stability and how they may interact in a crisis. Chapter 4 lays out three different pathways—provocation, entanglement, and information complexity—that could lead to escalation in this new environment. With this framework established, Chapter 5 dives into the key takeaways from the tabletop exercises. Finally, Chapter 6 provides key conclusions for this project and policy recommendations for managing the challenges identified.

In addition to this report, key elements and outcomes of our research project include:

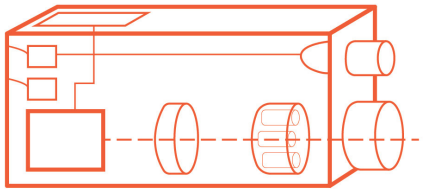
- **Tabletop Exercises:** CSIS carried out a series of eight tabletop exercises in 2019 that simulated crises between the United States and China and the United States and North Korea. During these exercises, participants were divided into "policy" and "technology" teams and tasked to design and approve a "collection plan" to improve SA drawing from a menu of emerging technologies, some of which, while providing useful information, could be considered highly provocative or intrusive. The insights from these exercises were used to inform the analysis in this report and our policy recommendations.

- **CSIS' "On the Radar" Website:** The site serves as a platform to report analysis and findings, share resources, and involve a diverse group of experts in the project. It houses primers on individual technologies, analysis of specific countries' strategic SA capabilities, and interactive tools to explore the project's analysis and assessments. (https://ontheradar.csis.org/)

- **Technology Primers:** These overviews explore emerging technologies and platforms—such as unmanned underwater vehicles (UUVs) for submarine detection, small satellites, and AI analysis applications—that will shape the future SA environment. (https://ontheradar.csis.org/issue-briefs/?brief_type=Tech%20Primer)

- **Country Profiles:** Analysis of country-specific developments and trends in strategic SA capabilities. (https://ontheradar.csis.org/issue-briefs/?brief_type=Country%20Profile)

- **Analysis:** "When Is More Actually Less? Situational Awareness, Emerging Technology, and Strategic Stability," is an analytical piece that provides initial observations and findings of this study. (https://ontheradar.csis.org/analysis/overview/)



2 | Understanding Situational Awareness Technologies and the Emerging Situational Awareness Ecosystem

The rapid expansion of new and existing technologies can provide opportunities for major breakthroughs in the ability to detect threats; track hostile actions and forces; process, interpret and communicate vast data sets; and predict and shape the actions and possibly even decisions of adversaries. Every technology has costs and benefits associated with its adoption, and the capabilities in the emerging strategic SA ecosystem are no different. Each of the emerging capabilities explored over the course of this project can be described using two separate categories: attributes for increasing strategic SA (discussed in this chapter) and risk factors that decrease strategic stability (addressed in the next chapter).

Platforms, Critical Enablers, and Defense and Counter Capabilities

The new technologies that will shape the strategic SA ecosystem moving forward can be divided into several broad categories. For the purposes of understanding and analyzing SA technologies and their effect on strategic stability, this study draws a distinction between "platforms" and "critical enablers." "Platforms," such as satellites, unmanned aerial vehicles (UAVs) or unmanned underwater vehicles (UUVs), or even microchip-enabled proximity cards, are the physical systems or structures necessary to access a collection target, carry a variety of sensor payloads, and support communications and data transmission from the sensor package. "Critical enablers," on the other hand, are the sensors, applications, or other technologies used to collect or analyze SA data many of which can be used on or in support of a variety of platforms. In the examples above, these would be the sensors attached to a UAV or the digital applications which collect and analyze data collected by those sensors. Technological advancement and innovation have been key to the development of both platforms and critical enablers. For example, advances in miniaturization, autonomy, robotics, and other technologies have led to the development of platforms that are smaller, more mobile and agile, and harder to detect. To better analyze the individual technology and the costs and benefits associated with employing it, platforms and critical enablers may be treated as a distinct for academic or theoretical purposes. However, in real-world scenarios, a critical enabler is useful only after its marriage with a platform that can put it into position to gather and process desired information.

Finally, in addition to platforms and critical enablers, this project also explored some strategic SA capabilities that may be termed "defense" or "countering." These capabilities contribute to the strategic SA ecosystem differently than most platform-critical enabler combinations: whereas most strategic SA capabilities focus on collecting information that can be used to inform decisionmakers during crisis or conflict, defense and countering capabilities either defend against adversary activities (for example, cognitive electronic warfare systems tasked with detecting, suppressing, and neutralizing adversary cyber intrusions) or seek to counter or degrade an adversary's strategic SA (such as through spoofing activities that can obfuscate an adversary's ability to perceive the operating environment). Together, defense and countering capabilities account for a small number of capabilities explored during this project, but such technologies may play an outsized role in escalation dynamics during future crises or conflicts given their potentially destructive nature and relevance to gray zone tactics.[26]

Key Attributes of Strategic SA Capabilities

To facilitate comparative analysis of a wide variety of technical capabilities and understand the enhancements they bring to strategic SA, the study team developed a common set of criteria or beneficial attributes that contribute to a highly effective strategic SA ecosystem. The six technical attributes are: vantage/range, speed, detectability, precision, persistence, and resiliency/reliability. Figure 2.1 defines each of these attributes and offers an example of a technical capability in which that attribute figures prominently.

VANTAGE AND RANGE

Vantage and range address the position within the physical operating environment from which new information can be gathered. While vantage focuses on the position from which information can be gathered (i.e., the position of the technology relative to the target being surveilled), range indicates

Figure 2.1 Emerging Technology Attributes

ATTRIBUTES		
ATTRIBUTES	**DEFINITION**	**TECHNOLOGY EXAMPLES**
Vantage/ Range	*The position from which new information can be ascertained.*	*Pseudosatellites that can position highly capable sensors outside of targetable distance.*
Speed	*The shortening of time between an adversary's action or decision to act, detection of that action, and the receipt of such by decision-makers.*	*Quantum computing that accelerates the ability to process and analyze vast data sets.*
(Un)detectability	*The degree to which an adversary can ascertain that information is being collected.*	*Advanced stealth capabilities that allow sensor platforms to evade detection by adversary air defenses.*
Precision	*The level of detail and quality of the information collected or a heightened degree of confidence in the information collected.*	*Synthetic Aperture Radar (SAR) that can track military movements despite weather and cloud cover.*
Smallsat	*The extent to which the capability can continuously collect data without gaps in coverage.*	*SmallSat constellations that can surveil specific areas for weeks or months.*
Resiliency/ Reliability	*The ability of a technology to employ redundant and robust systems for situational awareness in a contested environment.*	*Multi-sensor payload UAV swarms that can operate even if some of the platforms are destroyed or disabled.*

the operational "field of view" of the technology (i.e., the distance over which the capability can provide insight).

Some capabilities enable vantage benefits that were previously unattainable, inaccessible, or excessively costly or dangerous to attain. For example, high-altitude pseudosatellites provide a unique vantage to surveil adversaries, as their position between traditional UAVs and satellites provides a greater slant range without having to be directly over a target.[27] Elsewhere, plant-based sensors—an emerging SA technology that consists of physiology-based sensors capable of reporting the presence of various stimuli— could provide on-the-ground data collection that would otherwise require covert insertion, risky air drops, or other methods that could be considered violations of territorial integrity.[28] For example, these "smart plants" could be distributed either passively (e.g., via wind, wildfire, water, or animals) or actively (e.g., via mechanical or non-mechanical human activity).[29]

Range is related to vantage but refers specifically to the standoff distance afforded by the capability. Light Detection and Ranging (LIDAR) sensors can be calibrated to map ground structures through cloud cover using air or space assets that would have previously required flying at lower altitudes.[30] UUVs could be deployed inside safe territory and travel thousands of nautical miles to collect data.[31] China revealed its first large-displacement autonomous underwater vehicle (AUV), the HSU-001, in October 2019.[32] The U.S. Navy operates a limited number of UUVs primarily in a mine countermeasures (MCM) role, but it also has two major UUV developmental efforts underway: the Large Diameter UUV (LDUUV) and the Extra-Large UUV (XLUUV).[33] Both programs are still in early development and are not expected to shift to production until the mid-2020s.[34]

In any case, through enhanced range and vantage a state can optimize its ability to collect information at a distance, thereby minimizing risks of attack or sabotage to its own strategic SA assets.

SPEED

Whereas vantage and range denote a capability's advantageous position in space, speed refers to a capability's implications for time, namely the shortening of time between an adversary's action or decision to act, detection of that action, and the conveyance of information to the decisionmaker. Increased speed is a hallmark attribute of new technologies, driven by collectors' preferences for the rapid collection of more and more information to provide actionable options to decisionmakers.

Increased speed is a hallmark attribute of new technologies, driven by collectors' preferences for the rapid collection of more and more information to provide actionable options to decisionmakers.

Computer technologies that focus on data collection, analysis, or decision support are particularly relevant for "speed" given their ability to execute processes, detect changes in adversary systems, analyze large quantities of data, and quickly transmit the information across networks. Cyber surveillance capabilities can perform a wide variety of tasks and collect information at speeds that were previously unattainable. For example, they can intercept military leadership communications about troop movements, thereby shortening the time it would take to otherwise detect such actions. AI decision-support applications and quantum computing are comparatively newer technologies but could radically increase the speed at which decisions can be made or detected.

AI analysis applications are an example of a capability's potential to increase speed across multiple levels of strategic SA, including data collection, analysis, and decision-support tools. AI pattern recognition applications could sift through large amounts of data, including video, imagery, signal intercepts, and technical intelligence collected by strategic SA assets, and flag items of interest for analysts, thereby reducing the amount of time needed to analyze complex situations.[35] While many speculate that China may be gaining an edge in AI,[36] various press reports suggest that the United States currently has several major AI programs in development, including Project Maven and a classified pilot program reported by Reuters in 2018 focused on tracking the North Korean nuclear missile program.[37] Project Maven, a high-profile U.S military program, reportedly aims to use AI and machine learning to help intelligence analysts identify objects of interest from both moving and still imagery generated by the Unmanned Aircraft Systems fleet.[38] Although the mission of the latter program is classified, it is believed to focus on leveraging AI to monitor the North Korean nuclear program using satellite imagery to track mobile launchers, which can be difficult for human analysts to locate and track in real time.[39] Moreover, while available sources suggest that technology in North Korea is well behind that of South Korea, its rapid advances in cyber operations and information and communications technology suggest that it can be anticipated in the near future to develop machine learning and other types of AI technology and to apply those technologies in military affairs.[40] In a crisis involving compressed timelines, speed can be essential— information that arrives too late might as well not arrive at all.

DETECTABILITY

Detectability is the degree to which adversaries can recognize and identify surveillance activities targeting them. Certain capabilities such as advanced stealth surveillance aircraft may facilitate data gathering at reduced risk of detection. For instance, the United States is reportedly developing the RQ-180 Sentinel, a low-observable, unmanned HALE aircraft likely capable of active and passive electronic surveillance and electronic attack.[41] UUVs are an example of a currently-detectable capability that, given potential evolutions in related technologies (e.g., miniaturization, stealth, and quieting technology) stand to become increasingly difficult to detect.[42] Low detectability increases the ability to survey a target without detection, thereby collecting valuable information without the adversary's knowledge.

Even if an intrusion is detected, attribution can be a challenge. For example, given the nature of computer architecture, an adversary may find a cyber surveillance vulnerability and detect (or assume) a cyber intrusion but still be unable to determine what data is being surveilled. Advances in quantum computing may create scenarios where cyber surveillance is undetectable: recent research has demonstrated successful cloning of qubits, which may allow for undetectable, non-destructive, and non-intrusive hacking of both traditional and quantum computer systems.[43] According to various reports, the Reconnaissance General Bureau (RGB), North Korea's intelligence service, operates a number of hacking groups for which governments and cybersecurity companies attribute a variety of names (e.g., APT 38, Lazarus Group, TEMP Hermit, Hidden Cobra, APT 37, Group 123, Nickel Academy, Guardians of Peace, Silent Chollima, and Reaper).[44] Recorded Future, a cybersecurity firm, analyzed internet activity from territorial North Korea and found that little to no malicious cyber activity emanated from the North Korean mainland during the period observed, suggesting that North Korean state-sponsored cyber operations originated from locations outside of territorial North Korea, such as India, Malaysia, New Zealand, Nepal, Kenya, and Indonesia.[45]

PRECISION

Precision is defined as the level of detail and quality of the information collected or a heightened degree of confidence in the information collected. This attribute is particularly relevant for remote sensing capabilities, as more precise or detailed information is often the differentiating factor from older-generation technologies (more detailed optical sensors that provide higher-resolution photographs, for example). Advances in sensor technologies improve not only collection methods but also improve the value of the data itself in some cases. Whereas most mapping assets are typically restricted to either precision or volume, LIDAR's higher spatial sampling frequency can be dynamically changed to improve map accuracy at the cost of a lower data collection rate (measured in square kms/hr).[46]

Synthetic Aperture Radar (SAR) has been a core element of U.S. satellite surveillance capabilities for years, but until recently, such sensors were unable to image moving targets. Over the past two decades, however, advances in data-processing techniques have enabled SAR to both detect moving targets and determine their speed and direction of travel.[47] News reports suggest that a Chinese satellite constellation, Yaogan, employs both optical and SAR sensors and involves more than 50 satellites.[48] These advanced precision upgrades to SAR make the collected information more detailed and can contribute toward achieving important operational and strategic tasks such as tracking mobile missiles.

PERSISTENCE

Persistence is the extent to which a capability can continuously collect data by avoiding gaps in coverage. Persistence provides decisionmakers with important information that can give a clearer picture of a crisis or conflict over time, with fewer gaps in coverage, which in turn can greatly increase confidence levels. For example, HALE UAV pseudosatellites rate favorably for persistence because they could be capable of staying aloft for over three weeks, continuously monitoring a specific target and transmitting data the entire time.[49]

Current capabilities employed by the United States and China that are relevant to persistence include traditional HALE UAVs, a capability that provides persistence (but to a lesser degree than the potential of future pseudosatellites). China's People's Liberation Army (PLA) Navy operates the BZK-005 HALE UAV for maritime surveillance in the East and South China Seas, the Xiang Long HALE UAV, which could presumably be used in support of airborne early warning, and others.[50] The United States operates an extensive fleet of HALE UAVs, including the RQ-4 Global Hawk and the RQ-180. The RQ-4 Global Hawk has high-altitude surveillance capabilities similar to other assets but importantly offers persistent surveillance, with the ability to loiter for more than 34 hours.[51]

UUVs could also provide persistence: after being deployed directly into contested waters, UUVs can lie dormant until "awoken" by passing submarines, enabling the monitoring of areas through a latent capacity that was previously unachievable.[52] While the United States could be considered at the forefront of deploying UUVs to track detected submarines, the Chinese Academy of Science is reportedly carrying out research on unmanned maritime vehicles (UMVs) as well.[53]

RESILIENCY AND RELIABILITY

Resiliency and reliability refer to the ability of a capability to employ redundant, robust systems in a contested environment. The presence of a "back up" reduces the chances that a capability will "fail" in collecting useful information. Similarly, redundant, "swarmed" capabilities can "flood the zone" and confound the adversary's ability to target or disable the capability even if detected.

The United States has multiple efforts underway to develop "swarming" capabilities in which

small UAVs, numbering from just a few to potentially thousands, are networked together and share information to form the swarm's collective brain.[54] This collective brain then autonomously controls and directs the individual UAVs comprising the swarm in pursuit of the swarm's broader mission. If one or several drones are destroyed or debilitated, the swarm endures, as the collective brain compensates for the missing drones and then reorients. U.S. efforts to develop swarming capabilities are progressing along two main thrusts: disposable, air-launched micro-drones, which are roughly the size of a large hand, and small, reusable airborne UAVs which can be launched and recovered.[55] The effort to develop disposable, air-launched micro-drones, led by the Strategic Capabilities Office, successfully tested a swarm of 103 Perdix micro-drones in October 2016. Packed into flare canisters and ejected from an F/A-18 Super Hornet, the micro-drone swarm successfully "demonstrated advanced swarm behaviors such as collective decision-making, adaptive formation flying, and self-healing."[56]

Another form of resiliency can be seen in satellite constellations. Ranging from dozens to thousands, small satellite constellations improve the resiliency of the overall system to degradation due to natural causes, such as radiation damage, or adversary attacks.[57]

Surveying the Global Strategic SA Capabilities Landscape

Today, countries around the world possess varying degrees of strategic SA capabilities and continue to seek further advancements. The United States has extensive and mature strategic SA capabilities across all domains (air, land, maritime, space, and cyber) that help to characterize the operating environment, detect and respond to attacks, and discern actual attacks from false alarms across the spectrum of conflict, both conventional and nuclear. The U.S. military has always relied on these capabilities at the strategic level, but over the last 30-40 years, these capabilities have become more important at the tactical and operational level as technological advances have enabled more granular tracking and detection of enemy forces and communications, as well as coordination between different sensors and shooters, all with devastating effect. This combination of SA capabilities across all three levels of war and all domains has provided the United States unrivaled strategic SA and has become an essential component of U.S. military doctrine and planning. U.S. military superiority does not come from any stand-alone weapon system or platform, but its ability to integrate multiple C4ISR (command, control, communications, computers, information, surveillance, and reconnaissance) capabilities into a system-of-systems approach that translates strategic SA into kinetic and non-kinetic strike capabilities. The Navy's CEC/NFIC-CA capability is perhaps the best example of how several strategic SA systems, sensors, and platforms are integrated into a reconnaissance-strike complex with potentially devastating effect. If the United States wanted to target an adversary's capital ships—the most important ships in a fleet—it could send a stealthy F-35 to penetrate the enemy's air defense undetected and relay the enemy's location back to the carrier strike group; the strike group could then fire long-range anti-surface missiles at the enemy's capital ship without needing to get close.[58]

> *Military capabilities do not develop in a vacuum, and just as U.S. military planners recognized the value of integrating multiple systems, sensors, and platforms into a reconnaissance-strike complex, so too have American competitors.*

Northrop Grumman personnel conduct preoperational tests on a U.S. Navy X-47B Unmanned Combat Air System demonstrator aircraft on the flight deck of the aircraft carrier USS George H.W. Bush (CVN 77) May 14, 2013, in the Atlantic Ocean.

DoD photo by Mass Communication Specialist 2nd Class Timothy Walter, U.S. Navy/Released

Military capabilities do not develop in a vacuum, and just as U.S. military planners recognized the value of integrating multiple systems, sensors, and platforms into a reconnaissance-strike complex, so too have American competitors. The Chinese and Russians have developed sophisticated anti-access/area denial (A2/AD) capabilities that threaten to disrupt, degrade, or destroy essential U.S. C4ISR enabling capabilities. These advances are forcing military planners to rethink fundamental assumptions from the last 30 years about the near-guaranteed availability of C4ISR capabilities. Instead of establishing theatre-wide strategic SA superiority (e.g., U.S. operations in the 1991 Gulf War or Afghanistan and Iraq), the United States might only be capable of establishing temporary windows of C4ISR superiority for U.S. forces to operate from. U.S. military forces would work within these temporary windows of superiority to disintegrate enemy A2/AD systems and eventually re-establish theatre-wide strategic SA superiority, but this requires fundamental changes in U.S. training, doctrine, and force structures.[59]

China has invested and advanced considerably in its strategic SA capabilities. Although traditional shortcomings in its early-warning capabilities have been a major concern, the Chinese People's Liberation Army (PLA) today is poised to possess a more mature architecture that can enhance its capability to undertake nuclear counterattack and conventional operations. These range from space systems for electronic intelligence (ELINT) and remote sensing, including with aerial early-warning aircraft and unmanned systems, to a number of large, phased-array radars. In the years to come, China is likely to continue to redouble its efforts in response to new strategic requirements. For the PLA, the improvement of its capabilities for strategic early warning and SA will remain a challenge, but their efforts are starting to yield notable progress. Meanwhile, the PLA Rocket Force's new doctrinal emphasis on "rapid reaction" (快速反应) implies the capability for a rapid second strike, and China's posture could perhaps even evolve toward "launch on warning" (预警即发射), which would

demand significantly more reliable early-warning systems. The expansion of this global architecture in the years ahead will likely remain a priority as the PLA seeks to enhance its capabilities for power projection and joint operations.[60]

As the Chinese military is tasked with becoming "world-class" by mid-century, continued advances in its capabilities could enable the PLA to leapfrog ahead of the United States in certain domains and technologies. Seeking to establish itself as an "aerospace superpower" (航天强国), China has launched a range of satellites at a rapid pace, quickly expanding its space-based surveillance capabilities, including its capacity to rapidly process and glean insights from that data. The PLA has also emerged as a clear leader in experimentation with the use of unmanned systems for early warning and reconnaissance, fielding and integrating a growing number of systems that could increase its flexibility in enhancing SA in a crisis or conflict scenario. Meanwhile, PLA cyber capabilities could also contribute significantly to Chinese espionage.[61]

The PLA has also emerged as a clear leader in experimentation with the use of unmanned systems for early warning and reconnaissance, fielding and integrating a growing number of systems that could increase its flexibility in enhancing SA in a crisis or conflict scenario.

As the U.S.-China relationship becomes more competitive, even confrontational, these improvements in the PLA's strategic SA capabilities could prove stabilizing in certain respects but may also create new risks and challenges. For instance, improved strategic early warning could decrease Chinese anxieties about the risks of a "false negative" and enable more time for decisionmaking in a crisis in ways that mitigate the risks of accidental escalation. However, continued improvement of Chinese strategic early warning over the next decade or more could facilitate a transition to a posture of launch on warning that could prove risky or destabilizing, particularly if this trend corresponds with an increased reliance on complex emerging technologies to support these missions, such as AI. At the same time, these increases in capabilities will also improve the PLA's war-fighting capabilities in its near seas, including in likely conflict contingencies, while enabling future power projection. In this regard, these trends must be recognized as another dimension of China's emergence as a rival that can challenge traditional U.S. technological leadership.[62]

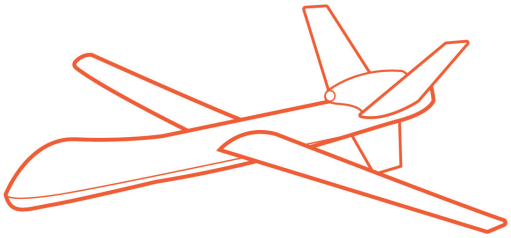
Unclassified sources contain little information on North Korea's C4ISR capabilities or strategic thinking. The country's leadership has expressed interest in signals intelligence (SIGINT), electronic warfare (EW), and asymmetric warfare since at least the armistice of the Korean War, during which Kim Il Sung employed SIGINT and communications intelligence (COMINT) abilities within the Ministry of Internal Affairs and the Reconnaissance Bureau for use against both foreign and domestic enemies. In addition, open-source reports have detailed alleged incidents of North Korean GPS jamming and spoofing dating back to 2010. North Korea is known to use its GPS jamming capabilities against South Korea, disrupting air traffic at Incheon and Gimpo International Airports. According to a report, there were four GPS jamming and spoofing attacks tied to North Korea between 2010 and 2016.

North Korean cyberattacks have also grown in sophistication over the last decade. According to South Korean intelligence agencies, North Korean cyber operations between 2005 and 2007 mainly stole data and documents from South Korean government agencies through individual email

accounts or agency websites. In 2005, the South Korean National Intelligence Agency found North Korean documents that ordered Lab 110 to "develop a hacking program to destroy the South's communication network and disguise the source of attack." These attacks were generally seen as rudimentary and simple. Since 2008, North Korea's cyberattack capabilities have started to focus on large-scale operations using complex malware. As North Korea's capabilities expanded, so did the range of targets: North Korean hackers have targeted government employees and institutions, researchers, cryptocurrency exchanges, banks, and media across the world. Until 2015, North Korean cyberattacks focused primarily on U.S. and South Korean government and financial organizations. However, in early 2016, North Korean hackers attempted to transfer $951 million from the Bangladesh Central Bank into North Korean-controlled accounts, the first of several subsequent North Korean attacks on banks around the world in 2017. American cybersecurity firm CrowdStrike assesses the speed of the North Korean hackers to be second only to Russian intrusion groups and superior to the Chinese.[63]

TWO STEPS FORWARD, ONE STEP BACK?

Emerging SA capabilities—characterized by the six attributes outlined above—will provide increased opportunities for strategic SA. Although the United States has traditionally been a frontrunner in SA capabilities, competitors such as China, Russia, and even North Korea are closing the gap. However, while these nascent capabilities may provide increased opportunities for strategic SA, they may also pose inadvertent risks to strategic stability.



3 | Risk Factors of Situational Awareness Technology and Strategic Stability

Advanced Strategic SA Capabilities and Stability Risks

Strategic stability generally depends upon the combination of the absence of incentives to use nuclear weapons first (crisis stability) and the absence of incentives to build up a nuclear force (arms race stability).[64] Schelling was the first to posit that crisis stability occurs "if neither side has or perceives an incentive to use nuclear weapons first out of the fear that the other side is about to do so."[65] Arms race stability, on the other hand, generally refers to a situation in which neither side has the incentive to augment their forces—qualitatively or quantitatively—based on the fear that their opponent could gain a meaningful advantage.[66] While strategic stability depends upon factors including successful crisis management, decreasing incentives to use nuclear weapons, and reducing incentives for longer-term arms races, this study focuses broadly on the escalatory pressures in crisis that could be influenced positively or negatively by the emerging strategic SA ecosystem- including those pressure points that could appear well below the nuclear threshold.

All the strategic SA capabilities considered in this study can, to some degree, introduce risks for strategic stability. These risks can be characterized as: intrusive, destructive, predictive, preemptive, dual-use, clandestine, vulnerable, and action-enabling. Like the attributes in the previous chapter, some risk factors are more common than others: for example, many technologies may be considered "action-enabling," as they enable military options that were previously difficult to achieve. The study team developed and used a set of stability risk factors to evaluate the extent and manner in which escalatory risk—either in terms of creating incentives for escalatory military action that might prove uncontrollable or increase the likelihood of miscalculation with escalatory outcomes—could be associated with emerging SA capabilities. These risk factors are elaborated upon in Figure 3.1. This common set of criteria allowed for more consistent comparisons across the range of different technologies in terms of evaluating their risk potential. Figure 3.1 defines each of these escalatory risk factors and provide illustrative examples.

Figure 3.1: Risk Factors Associated with Emerging SA Technologies

RISK FACTORS		
STABILITY RISK FACTOR	**DEFINITION**	**TECHNOLOGY EXAMPLES**
Predictive	*The degree to which a capability allows a state to anticipate adversary actions as opposed to merely reacting to them after they are completed.*	*AI decision support tools that examine patterns of behavior and detect anomalies to improve the accuracy and timeliness of warning.*
Preemptive	*The extent to which a capability enables acting against adversary actions or plans before they can be completed.*	*Air, ground, or sea-based sensors that can detect the movement of mobile missiles prior to launch.*
Action-enabling	*The degree to which a capability enables new military options.*	*Cyber exploit that can identify and (if desired) disable network or space-based capabilities; or unmanned air or maritime surveillance capabilities that can identify and locate adversary capabilities and provide real-time targeting.*
Intrusive	*The extent to which a capability must enter an adversary's territory, airspace, or networks.*	*An autonomous UUV or UAV with advanced sensing capability deployed inside adversary territory, airspace, or waters.*
Destructive	*The extent to which a capability can disable or degrade an adversary system, either temporarily or permanently, in achieving its objective.*	*A cyber exploit that can detect a decision message by an adversary and disrupt or alter the message at the same time.*
Clandestine	*The extent to which capabilities derive significant military advantage by being kept secret and pose significant disadvantage if revealed.*	*Use of covert personnel or capabilities to deploy highly advanced sensing capabilities in adversary territory.*
Vulnerable	*The degree to which an adversary can deny the use of a capability.*	*Air, maritime, or space surveillance assets that are vulnerable to shoot down, spoofing, or blinding.*
Dual-use	*The extent to which a capability is used for conventional and nuclear missions.*	*Space-based surveillance or communications systems that support both conventional and nuclear missions.*

Assessing Risk in the Emerging Strategic SA Ecosystem

PREDICTIVE, PREEMPTIVE, AND ACTION-ENABLING

Predictive, preemptive, and action-enabling capabilities are similar in that their escalatory risks are associated with the collection of certain information that could incentivize military actions through a perceived offensive advantage. Such actions are wide ranging but could include the collection of information that enables or encourages offensive first-mover actions (such as precision targeting of dual-use delivery systems) or defensive actions that could be perceived as escalatory if detected by the other side (such as dispersing nuclear weapons to improve survivability in a damage-limitation strategy). While all three risk factors are closely related, emphasizing their differences is important for understanding how they may independently impact strategic stability.

PREDICTIVE

Predictive risk factors describe the degree to which a capability allows a state to anticipate adversary actions in advance as opposed to merely reacting to them after they are initiated. Predictive technologies could potentially provide insight into the movement of adversary forces, the deployment of weapons systems, or even adversary intent to initiate military conflict before such actions would otherwise be perceived by traditional strategic SA capabilities (e.g., early-warning satellites designed to detect missile launches post-launch). Even if a predictive capability does not provide specific targeting information, it may prompt decisionmakers to act in an anticipatory fashion, diplomatically or militarily. On the other hand, when faced with predictive capabilities, the targeted country may feel increased "use or lose" pressures that could lead to escalatory outcomes. Decisionmakers could also use information collected by predictive capabilities to further enhance their strategic SA in concert with other capabilities. For example, if a predictive technology detected that an adversary is likely to take an action (e.g., fueling missiles in preparation for launch), decisionmakers could employ other capabilities to surveil the area and improve certainty (e.g., focusing satellite sensors on launch pads to verify missile launch preparations).

Even if a predictive capability does not provide specific targeting information, it may prompt decisionmakers to act in an anticipatory fashion, diplomatically or militarily.

The predictive nature of AI technologies is representative of the challenges associated with such capabilities. For example, predictive analytics applications could ingest large amounts of data and discover previously unknown but strategically relevant anomalies, enabling more accurate and timely information for analysts.[67] While obviously advantageous for the state employing such a capability, the predictiveness of such a system could pose stability risks. Analysts using such an application could potentially predict the mobilization of forces or planning for a snap invasion by a competitor, incentivizing a military response before the window of opportunity closes. .[68]

PREEMPTIVE

Preemptive capabilities not only anticipate adversary action, but also enable disruptive responses to adversary actions or plans before they can be completed. While similar to predictive risk, preemptive capabilities can exist independently from one another. For example, while AI analysis applications may provide predictive insight into adversary actions, such a capability would not be preemptive if it does not provide incentive and opportunity to counter the action before it is completed.

On the other hand, a UAV deployed to monitor an adversary's mobile missiles would be a preemptive capability if it were able to detect mobile nuclear missiles moving out of garrison and enable actions to disrupt the missile deployment, such as destroying the missiles themselves or destroying the road to limit their movement.

Preemptive actions could also be defensive in nature but may be viewed as offensive and escalatory by the adversary, given the nature of security dilemma dynamics.[69] One example of this risk factor would be moving one's own nuclear weapons to maintain second-strike capability in response to information that an adversary is surveilling such assets. While such an action is defensive as it relates to protecting one's own forces, it would in effect be preempting an adversary's (potential)

actions against said forces, which could in turn incentivize the adversary to strike before the weapons have been moved, thus risk upending strategic stability.

ACTION-ENABLING

The final risk factor most closely associated with predictive and preemptive capabilities is "action-enabling," or the degree to which a capability enables new military options. This risk factor is perhaps the most intuitively destabilizing, as military options can risk escalating a crisis into a full-blown conflict or escalate a conflict from the conventional to the nuclear level. A capability that is either predictive or preemptive may enable further information collection or simply provide insight into an adversary's forces, whereas action-enabling capabilities inherently enable military options.

Spoofing is an example of an action-enabling capability that could create escalatory pressures during crisis or conflict. Spoofing (a form of electronic attack where the attacker tricks a receiver into believing a fake signal, produced by the attacker, is a genuine signal) could be used to take control of a satellite by successfully spoofing the command and control uplink signal.[70] If the satellite being spoofed is used for both conventional and nuclear missions and the adversary is unable to discern the intent of the attack, it may raise the perceived stakes in a crisis and lead to escalation.

INTRUSIVE

The intrusive risk factor describes the extent to which a capability must enter an adversary's territory (land or maritime), airspace, or networks to accomplish its task. This action may be viewed as a risk to strategic stability. Intrusive capabilities often violate traditional concepts of territorial sovereignty and provide opportunities for misperception of intent. Examples of intrusive capabilities include UAVs that violate adversary airspace, UUVs that loiter near adversary submarine bases, or the placement of compact, multisensor proximity devices near land targets (potentially placed by SOF inserted into adversary territory).

In addition to these examples of intrusive capabilities in the traditional sense (violating territorial sovereignty), cyber surveillance capabilities can also be considered intrusive, as they violate private networks that transmit sensitive communications. This poses risks to strategic stability, as the collected information can concern either conventional or nuclear forces and the targeted state may be unable to discern what type of specific information is being collected. If decisionmakers believed their NC3 was being electronically monitored, this could lead to escalation in crisis scenarios.

DESTRUCTIVE

Destructive risk factors describe the extent to which a capability can disable or degrade an adversary system, either temporarily or permanently, in pursuit of its information gathering objective. This risk factor is uncommon in the strategic SA capabilities explored in this project, as such capabilities are primarily concerned with collecting information rather than degrading adversary capabilities, but some strategic SA capabilities can be destructive in the course of their information collection. For example, a cyber surveillance exploit that can monitor adversary communications could also be destructive if it were able to alter, disrupt, or delete messages between high-level government and military leaders. Such actions may endanger strategic stability if an adversary perceived that electronic tampering was intended to disrupt communications with their nuclear forces, hinder the execution of nuclear operations, or stall reactions to an imminent nuclear strike.

Defense and countering strategic SA capabilities are also inherently destructive to some degree, as they seek to degrade adversary systems or defend against threats and thus neutralize attacks. Satellite jamming is an example of a destructive strategic SA capability in which an electronic anti-satellite (ASAT) attack interferes with radio frequency communications by generating noise in the same frequency band and within the field of view of the antenna on the targeted satellite or receiver. While not as destructive as kinetic ASAT weapons, satellite jamming can disrupt adversary communications and degrade their ability to function, which could cause escalation during a crisis scenario. This dynamic could threaten strategic stability, especially if the satellites targeted by jamming are dual use (used for conventional and nuclear missions) and adversaries are unable to discern intent (see section on entanglement, Chapter 4.2)

CLANDESTINE

If a capability is clandestine, it derives significant military advantage from being kept secret but also can pose significant disadvantage and risk if revealed.[71] DOD doctrine defines clandestine activities as "operations sponsored or conducted by governmental departments in such a way as to assure secrecy or concealment" that may include relatively "passive" collection and information gathering operations.[72] If a technology is clandestine, it means that it is "hidden," where the aim is for it to not be noticed at all. In contrast, covert means "deniable," such that if the technology is noticed, it is not attributed to a group.[73] For example, plant-based sensors can be classified as clandestine, as they could be deployed on adversary territory; an adversary aware of deployed plant-based sensors would remove them, block their ability to report, block their ability to detect, or avoid the limited range of detection these plant-based sensors would have. However, successfully deployed modified plants would be very hard to identify in an environment, and their existence may be unknown. Adversaries who discover plant-based sensors in their territory may not be able to immediately identify who deployed the smart plants as the biological material would not necessarily have any perceptible human or technological trace.[74]

VULNERABLE

In addition, vulnerability of SA technologies—defined as the degree to which an adversary can deny the use of a capability—is another risk to strategic stability. Technological vulnerability—the chance of failure of an entire technological system due to outside events—is in stark contrast to when a technological system can be said to be resilient (i.e., if it can maintain its purposes in the face of a threat).[75] Adversaries are likely to disrupt or destroy strategic SA capabilities that are more vulnerable, thereby cutting off the flow of information. For instance, emerging technologies for SA in the air, maritime, or space domain could potentially be vulnerable to shootdown, spoofing, or blinding.

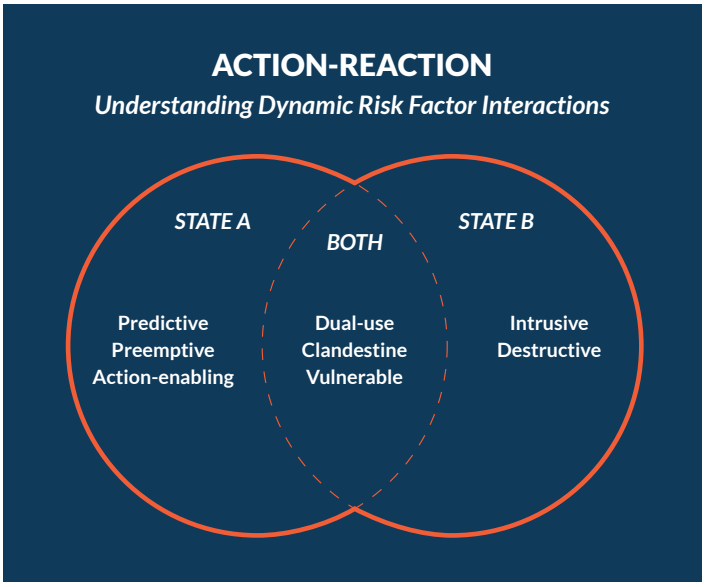
DUAL-USE

Dual-use capabilities are those that are used for both conventional and nuclear surveillance or warning missions. The dual-use nature of emerging technologies can create confusion as to the intentions of the surveilling party. For example, if UUVs are used to observe an adversary's conventional submarines (SSNs), which might be housed alongside its nuclear-armed ballistic missile submarines (SSBNs), the surveilled state would be unable to tell which assets were being targeted and may deem their nuclear assets as under threat. Dual-use capabilities may further upset strategic stability vis-à-vis the escalation pathway of entanglement (explored in Chapter 4).

Action-Reaction: Understanding Dynamic Risk Factor Interactions

As shown in Figure 3.2, escalation plays out dynamically between two or more actors in a crisis, each managing their own perception of risk and reacting to the actions of the other. The risk factors described above can interact in unique and complex ways as actors weigh the costs and benefits of using capabilities to increase their strategic SA relative to an adversary. In some cases, these risks manifest as a perception that escalation can be managed on reasonably favorable terms; in other cases, they manifest as a misunderstanding of the other actors' intentions. The following Venn diagram suggests how the pursuit of information dominance by a hypothetical "State A" employing a strategic SA capability may create both first-mover and miscalculation risks relative to the target, "State B."

Figure 3.2: Action-Reaction Dynamics among Risk Factors



This dynamic can be illustrated with an example scenario, such as the deployment of a HALE UAV over adversary territory. In this example, State A introduces an intrusive risk to which State B may feel compelled to respond to militarily, either because it perceives the violation of its territory as an act of war itself or because it believes the surveillance is a precursor for attack by State A. The UAV deployment, if successful, can introduce a preemptive or action-enabling risk by producing information that incentivizes State A to escalate militarily in hopes of capturing a strategic advantage or terminating the conflict before State B is able to take further action. Such first-mover incentives may be viewed by State A as controllable or conventional, at least initially, which may contribute to their appeal. On the other hand, the HALE UAV is vulnerable, since it is detectable and easily targeted with advance air defense assets. If it is targeted by State B and shot down, State A chooses whether to accept the loss or escalate—in essence, drawn into further conflict by an intrusive and vulnerable asset.

Another example, such as a cyber exploit used to surveil adversary networks, could pose risks of misperception for both states involved. In this hypothetical scenario, State A employs an intrusive and potentially destructive exploit into State B's networks. The information gained may be preemptive or even predictive if AI programs are used to analyze the large amounts of data collected. State A may view the exploit as maintaining a "baseline" of surveillance given the constant back and forth common in cyber competition today, but should the clandestine surveillance be detected, State B may question the intent of such surveillance (especially if the network is dual use and used in both conventional and nuclear missions). This scenario is plausible given publicly available military doctrine. For example, the 2018 DOD Cyber Strategy

This interplay of risk factors can contribute to our understanding of how the pursuit of information dominance may contribute to escalation, either by incentivizing first-mover actions or by heightening miscalculation risks during crises between nuclear-armed adversaries.

outlines an official "defend forward" doctrine that aims to "disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict."[76] This poses risks to strategic stability, as the probing may be intended for defensive measures (collecting information about cyber threats to stop them before they can be employed against U.S. targets), but the targeted state may perceive the action as a threat to either conventional or nuclear missions, particularly during a crisis.

This interplay of risk factors can contribute to our understanding of how the pursuit of information dominance may contribute to escalation, either by incentivizing first-mover actions or by heightening miscalculation risks during crises between nuclear-armed adversaries.

Risk Versus Reward: Evaluating Strategic SA Capabilities

The study team examined 28 different technical capabilities with application to strategic situational awareness in terms of both their key attributes and their potential stability risks. These technical capabilities were presented during tabletop exercises. Figure 3.3 outlines the technologies explored by this project. The table is not exhaustive, but it represents strategic SA capabilities across all domains and is representative of the emerging SA ecosystem.

Which Technologies Were Explored During On the Radar?

SEA AIR LAND
SPACE CYBER DEFENSE/COUNTERING

P = PLATFORM
CE = CRITICAL ENABLER

STRATEGIC SA CAPABILITY	DOMAIN & TYPE	DEFINITION	EXAMPLE OF STRATEGIC SA APPLICATION	DEMONSTRATIVE TECHNOLOGY	DOMINANT ATTRIBUTES	DOMINANT RISK FACTORS
Autonomous Unmanned Underwater Vehicle (UUV)	P	Sea-based sensor platform with little to no human input	Employed to track submarine and surface vessels	Large Diameter UUV (LDUUV)	Vantage/ Range, Persistence	Intrusive, Preemptive
Unmanned Underwater Vehicle (UUV) Swarms	P	Groups of UUVs networked together	Swarms to specific submarine or surface vessel target (including ports)	Aquabotix UUV Swarm	Persistence, Resiliency/ Reliability	Intrusive, Action-enabling
Unmanned Underwater Vehicle (UUV) Nets	P	UUVs deployed to passively monitor geographic chokepoints	Static/slow-moving UUVs deployed to littoral waters/geographical chokepoints to track submarineand surface vessel activity		Persistence, Precision	Preemptive, Clandestine
Unmanned Surface Vehicle (USV)	P	Unmanned surface platform capable of being underway for weeks on end	Used to patrol, track, and deploy a range of smaller USV and UUV systems	U.S. Navy Autonomous Swarmboats; Aquabotix USV Swarm	Vantage/ Range, Precision	Intrusive, Vulnerable
High Altitude Long Endurance (HALE) UAV	P	Unmanned aerial vehicle with wide range of sensor capabilities	Surveil adversary capabilities at high-altitude and maneuverable to lower altitudes	RQ-4, RQ-180	Vantage/ Range, Precision	Intrusive, Vulnerable
High Altitude Pseudosatelites	P	Extremely high-altitude UAVs with length-ened wingspan able to surveil an area of interest for days to weeks	Provides long-term, persistent coverage of land and surface targets from over 65k feet in altitude	Airbus Zephyr; Boeing PhantomEye	Vantage/ Range, Persistence	Intrusive, Vulnerable
Unmanned Aerial Vehicle (UAV) Swarms	P	Groups of UAVs networked together to surveil targets in close proximity	Deployed to surveil land and sea targets at short distance	DARPA Gremlins Program	Vantage/ Range, Resiliency/ Reliability	Intrusive, Action-enabling
Unmanned Underwater Vehicle (UUV)-Launched Unmanned Aerial Vehicle (UAV)	P	Small UAV deployed from UUV with limited optical sensors and comms capabilities	Designed to take aerial images of coastal targets in close proximity		Speed, Precision	Intrusive, Preemptive
Autonomous Unmanned Aerial Vehicle (UAV)	P	Next-generation unmanned aircraft with both reconnaissance and warfighting capabilities	Provides aerial imaging and real-time reconnais-sance over land and sea targets	Predator MQ-1, MQ-9, MQ-X	Vantage/ Range, Precision	Intrusive, Vulnerable, Dual-use
Manned, Next-Gen Stealth Aircraft	P	Next-generation manned stealth aircraft equipped with optical sensors	Performs high-altitude reconnaissance missions of and and sea targets	Lockheed TR-X	Speed, (Un)detectability	Intrusive, Dual-use
Smallsat Constellations	P	Small satellites networked together to surveil target	Employs advanced sensors from space to surveil targets	SensorSat	Persistence, Resiliency/ Reliability	Preemptive, Dual-use
Co-Orbital Reconnaissance Satellites	P	Small satellites placed in a similar orbit to their target	Tracks and monitors space-based adversary capabilities including satellites used for surveillance, communications, and early warning		Vantage/ Range, Persistence	Dual-use, Clandestine
Quantum Computing	P	Computers that take advantage of physics at the quantum level	Enables increasingly rapid data analysis as well as processing power for increasingly autono-mous systems	China's National Laboratory for Quantum Information Science	Speed, (Un)detectability	Predictive, Action-enabling
Artificial Intelligence (AI) Analysis applications	CE	Computer applications to support human analysts and decision-makers	Reconciles diverse data streams to rapidly provide pattern recognition and anomaly detection tools to analysts	Project Maven	Speed, Precision	Predictive, Vulnerable
Cyber Surveillance	CE	Software and hardware that provides access to an adversary's computer network	Provides insight into adversary behavior, intentions, and decision-making	Eternal Synergy and Double Pulsar	(Un)detectability, Persistence	Intrusive, Clandestine

Which Technologies Were Explored During On the Radar

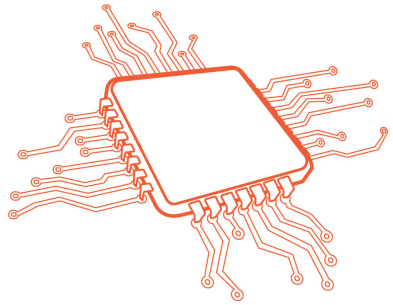
(continued)

SEA AIR LAND SPACE CYBER DEFENSE/COUNTERING

P = PLATFORM

CE = CRITICAL ENABLER

STRATEGIC SA CAPABILITY	DOMAIN & TYPE	DEFINITION	EXAMPLE OF STRATEGIC SA APPLICATION	DEMONSTRATIVE TECHNOLOGY	DOMINANT ATTRIBUTES	DOMINANT RISK FACTORS
Compact, Multisensor Proximity Devices	CE	Credit-card sized secure, low-resolution wireless sensors	Passive sensors placed close to land target location. Example target includes nuclear fuel fabrication facilities		Precision, Persistence	Intrusive, Clandestine
Plant-based Sensors	CE	Physiology-based sensors capable of reporting the presence of various stimuli	Employed in adversary territory to monitor for certain chemical or radiological signatures associated with activities of interest	DARPA Advanced Plant Technologies Program	Vantage/ Range, (Un)detectability	Intrusive, Clandestine
Light Detection and Ranging (LIDAR)	CE	A sensor that generates spatial data from light reflected from a laser	Rapidly 3D maps a target area from air, space, or the surface of the ocean with potential tracking capabilities	DARPA HALOE	Precision, Persistence	Dual-use, Preemptive
Hyperspectral Sensors	CE	Takes hundreds or thousands of contiguous images in narrow wavebands	Provides a picture of adversary behavior using hyperspectral images that cut through obstacles to optical sensors	ACES-Hy UAV sensor	Vantage/ Range, Precision	Dual-use, Preemptive
Non-acoustic Submarine Detection	CE	Detection technologies including light-based imaging and magnetic detection	Magnetometers, in particular, are used to attempt to track adversary submarines	China's Guanlon Project	Vantage/ Range, Precision	Clandestine, Action-enabling
Remote Radiation Detection by Electromagnetic Air Breakdown	CE	Uses the reflection of high-intensity pulses to probe the concentration of charged species produced by ionization in air	Used to detect nuclear activity in facilities across the fuel cycle.		Vantage/ Range, Precision	Intrusive, Preemptive
Electro-Optical (EO) Sensor	CE	Use lenses and mirrors to image objects across the electromagnetic spectrum	Used to detect and track aircraft, missile launch warning, target acquisition and surveillance, etc.	ARGUS	Vantage/ Range, Precision	Dual-use, Preemptive
Gravity Gradiometer	CE	Passive sensor that measures minute differences in the earth's density	Yields information on geologic structures underground and undersea used to surveil tunneling by adversaries		Vantage/ Range, Precision	Dual-use, Preemptive
Synthetic Aperture Radar (SAR)	CE	Radar-based sensor used to build high-resolution imagery from mobile platforms	Used to surveil and detect land-based assets such as mobile missiles	RADARSAT-2	Precision	Dual-use, Preemptive
Inverse Synthetic Aperture Radar (ISAR)	CE	Uses movement of the target to generate high-resolution images	Able to image moving objects from a variety of vantage points		Precision	Dual-use, Preemptive
Cognitive Electronic warfare		Uses AI to enhance development and operation of electronic warfare technologies	Used in attempt to detect, suppress, and neutralize cyber attacks		Speed, Persistence	Predictive, Clandestine, Destructive
Spoofing		Cyber attack in which attacker masquerades as legitimate user and provides false data to the system	Can be used to take control of a satellite or inject corrupt data into communications or otherwise poison data from SA sources		Vantage/ Range, Precision	Intrusive, Action-enabling, Destructive
Satellite jamming		Electronic anti-satellite (ASAT) attack that interferes with communications traveling to and from a satellite (downlink and uplink)	Can be used to disrupt missile warning systems, SIGINT, GPS, and communications satellites	Krasukha-2, Zhitel, and Borisglobesk	Persistence, Resiliency/ Reliability	Action-enabling, Destructive



4 | Pathways to Escalation

Of particular concern are three potential escalation pathways—provocation, entanglement, and information complexity—that may be triggered or exacerbated by the use of emerging strategic SA-enhancing capabilities. Although multiple pathways may be activated during an actual crisis, either simultaneously or sequentially, examining each of these escalatory pathways individually provides insight into the interplay of strategic SA technologies and stability risks.

Provocation

The active nature of the emerging strategic SA ecosystem means that states have the capability to penetrate adversary territory (via land, sea, and air) and networks to gain increasingly precise and potentially actionable information. However, the use of these capabilities risks discovery and response by the state under surveillance. Likewise, these capabilities may generate information that suggests the opening of an offensive window of opportunity, greatly increasing incentives to move first. Escalation through provocation occurs when parties to a crisis lack an ability to determine the offensive or defensive intentions behind a proposed action or information collection effort, greatly intensifying escalatory pressures. It may occur because:

- information collection efforts begin to influence rather than observe the course of a conflict or crisis (whether intentional or not) through intrusive or disruptive activity; or
- the rapid, precise, and persistent nature of SA capabilities creates opportunities or incentives to take action on a preemptive or preventive basis.

In other words, a provocation-based escalation cycle occurs when the use of these technologies is perceived in offensive terms by the country being observed (e.g., by illegal territorial intrusion) or the strategic SA capabilities afford a significant offensive or first-mover advantage to the observing state.

These provocation dynamics could play out through several different scenarios:

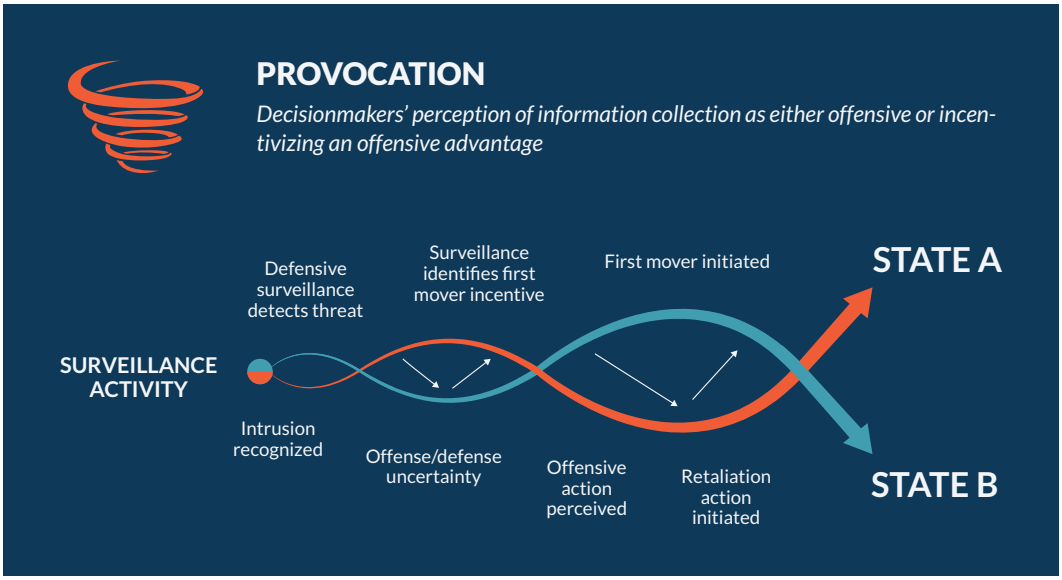
1. The use of intrusive technologies challenges legal and political concepts of sovereignty and is perceived as offensively intended (a territorial incursion can be perceived as an act of war regardless of its defensive intent);
2. The intended mission of these capabilities (general surveillance versus counterforce support or surveillance versus strike) is not readily identifiable and is misperceived;

3. Surveillance capabilities intentionally or unintentionally approach vital strategic assets as they conduct surveillance and therefore provoke a response;

4. Clandestine capabilities, such as active cyber surveillance, are discovered, prompting surprise and uncertainty as to risks and damage; and

5. Surveillance capabilities initiated for defensive purposes identify preemptive or action-enabling options, prompting a willingness to take an escalatory offensive action in hopes of terminating the crisis on favorable terms. Or, if the surveillance is detected or revealed, the country under surveillance may assume such intentions and undertake an escalatory step of its own.

Figure 3.2: Action-Reaction Dynamics among Risk Factors



OBSERVING VERSUS SHAPING

The very act of collecting information could provoke an escalatory response because many emerging systems are intrusive and may operate in ways that are perceived to violate state sovereignty. This may occur from the violation of internationally recognized or unilaterally proclaimed borders, territorial waters, and sovereign airspace but could also provoke a response by intruding in the far less well-defined and legally delineated domains of cyber and space.

If clandestine information gathering assets—such as cyber intrusions or unmanned systems believed to be stealthy—are discovered by an adversary operating within its territory, they could be indistinguishable from a destructive or offensive attack and be considered provocative. There

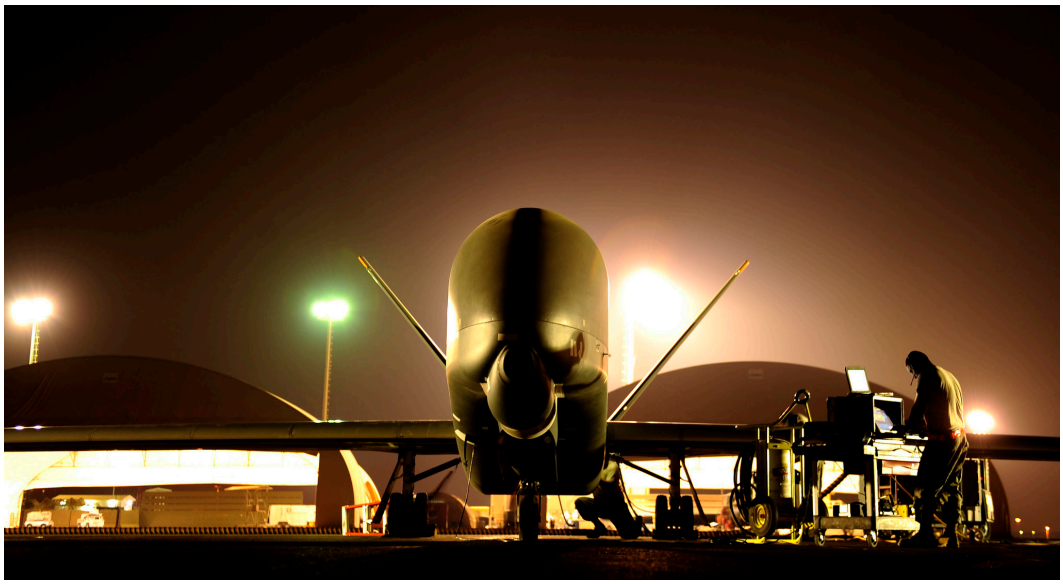
The very act of collecting information could provoke an escalatory response because many emerging systems are intrusive and may operate in ways that are perceived to violate state sovereignty.

is reason to believe assets used solely for information collection could nonetheless appear threatening to an adversary and provoke the use of force. As Robert Jervis and Mira Rapp-Hooper have written, "there is an all-too-human tendency to assume that an action will be seen as it is intended to be seen."[77] Nonetheless, as John Mearsheimer has recognized, "uncertainty about the intentions of other states is unavoidable," and "states can never be sure that other states do not have offensive intentions."[78] Inherent in the logic of a security dilemma is that states tend to view their own measures as defensive while interpreting those of other states as threatening.[79] In addition to intentions, states can also misperceive capabilities.[80] It seems likely that states would be susceptible to mischaracterize the purpose of SA assets as well, especially if they operate close to vital strategic assets as they conduct surveillance.

The role of unmanned systems in complicating perceptions of risk and provocation deserves particular attention, in part because of their increasing use. For the surveilling country, the use of unmanned assets might prove appealing due to the lack of risk to human life and lower perceived consequences of a loss. However, the surveilled country may perceive lower risks associated with attacking or disabling intrusive unmanned platforms and thus initiating an escalatory response. Also, technological developments that reduce the vulnerability of systems might both encourage intrusive uses and potentially make it difficult for adversaries to distinguish them from armed or offensive platforms, especially if surprised or spooked by the discovery of the intrusive or clandestine capability. For example, UAV platforms with low-observability characteristics might be employed in denied airspace, particularly in contexts in which an adversary has limited tools to detect an intrusion. UAVs are already used extensively for both SA and kinetic purposes, with few visible distinctions between armed and unarmed systems.[81] The use of surveillance drones has become so ubiquitous across conventional crisis and conflict, including counterterrorism operations, that decisionmaking procedures may lack guidance regarding their use under a nuclear shadow.

History provides some indication of how these escalatory dynamics may play out with unmanned systems. Pakistan has publicly denounced U.S. UAV missions in its airspace, objecting to any violation of state sovereignty.[82] In June 2019, Iran shot down an unmanned U.S. Navy RQ-4 Global Hawk surveillance aircraft, claiming it had been operating over its airspace—a claim disputed by U.S. officials.[83] This reportedly prompted planning by the United States for strikes against Iranian military facilities—an effort that was apparently called off at the last minute by the president.[84] Unmanned naval and subsurface systems, which could be used for intrusive operations in adversarial territorial waters or in contested areas, pose similar provocational challenges.

The cyber realm is another area particularly vulnerable to the provocation pathway, in large part because it can be especially challenging to delineate between offensive and defensive intentions in the cyber domain. The line between surveillance and attack is very thin, as techniques that would be useful to launch cyber probes mirror those of an offensive attack. Cyberattacks are often latent, and operations that are intended solely for espionage can sometimes transition to offensive purposes by adding onto the initial intrusion with malware modules.[85] Moreover, because cyberattacks may have unpredictable effects and are particularly prone to misestimations of "what the other side



U.S. Air Force maintenance technicians conduct preflight checks on an RQ-4 Global Hawk unmanned aerial vehicle assigned to the 380th Expeditionary Operations Group at an undisclosed location in Southwest Asia Nov. 23, 2010.

DoD photo by Staff Sgt. Andy M. Kin, U.S. Air Force/Released

thought it was doing," there is significant potential for misunderstanding and miscalculation.[86] The repercussions of this during peacetime might be limited, but during a crisis between nuclear-armed powers, there are risks that cyber surveillance targets could perceive an intrusion into their networks as a precursor to an attack. Compounding these potential misperceptions is the fact that there does not appear to be clearly defined differences between offense and defense across the cyber strategies of different countries.[87] The traditional nature of offense and defense in cyberspace is often different from that of the kinetic domains, and the intentions behind specific cyber operations—whether to protect one's own information or obtain access to another's—may be divorced from the tactics themselves.[88] Indeed, across the techniques of many cyber operations, the basic difference between surveillance and attack is "essentially a difference in intent."[89] Thus, what one party sees as cyber surveillance could appear highly aggressive and provoke escalation.

The cyber realm is another area particularly vulnerable to the provocation pathway, in large part because it can be especially challenging to delineate between offensive and defensive intentions in the cyber domain.

Of course, the capability to monitor activities associated with nuclear weapons could also prove highly stabilizing as a means of confirming assurances of non-aggressive intent, providing verifiable transparency and reducing risks of surprise while creating space for diplomacy and other tools to assist in de-escalating the crisis. That would require careful thinking about the relative value of covert versus overt techniques and the diplomacy and messaging associated with the use of potentially provocative surveillance capabilities.

INCENTIVES AND OPPORTUNITIES FOR PREEMPTIVE OR PREVENTIVE ACTION

As conventional SA capabilities become more useful for nuclear warning, tracking, and targeting missions, both their utility to the surveilling country and perceived risk to the surveilled country grows.[90] While transparency of strategic-level capabilities has a stabilizing effect among great powers with credible second-strike survivability (and thus, mutually assured destruction), in dyads with significant nuclear asymmetry, greater knowledge of the location of the smaller country's strategic assets could undermine stability by shifting incentives for both countries toward using nuclear weapons first.[91] As Thomas Schelling observed, "the reciprocal fear of surprise attack" could destabilize a crisis and produce a war undesired by both parties.[92] Indeed, in crisis scenarios involving both conventional and nuclear weapons, game theoretic modeling suggests that developments that improve the capabilities of conventional forces to target nuclear assets are inherently destabilizing.[93]

Existing HALE UAV assets, for example, were originally intended for contingency and conventional wartime operations. However, they could also be useful to track a small country's nuclear mobile missiles or surveil for other warning indicators, such as the movements from garrison, changes in pattern of life, or the generation of forces. Constellations of small satellites could also offer the capability for real-time, continuous, high-definition visual and infrared imaging of areas of interest.[94] In conjunction with airpower, cruise missiles, and other conventional strike assets, such high fidelity surveillance capabilities may provide operators formidable capabilities for locating and engaging a range of targets.[95] Improved precision and coverage of surveillance technology is eroding the security that mobility once provided to survivability.[96] More broadly, U.S. intelligence capabilities for eroding second-strike forces are very advanced, according to some estimates, creating vulnerability for its second- and third-tier nuclear adversaries.[97]

For the targeted state, the ability of adversary strategic SA capabilities to inform or enable preemptive or preventive action may make it increasingly challenging to effectively conceal nuclear forces.[98] In such cases, the actual or perceived ability of the more technologically advanced country to carry out precision-strike missions against strategic nuclear assets will make any SA-enhancing activities—even those purely defensive in nature—seem highly provocative or escalatory. For example, if North Korea knew or suspected that the United States had the capability to track and destroy its nuclear mobile missiles, it might assume that any U.S. intelligence, surveillance, and reconnaissance assets in its airspace were a threat to its nuclear assets regardless of their actual assigned mission. Thus, highly intrusive surveillance assets could provoke escalation by creating pressure for the smaller nuclear power to "use or lose" its nuclear weapons and "posture its forces for an early use in a crisis, before its nuclear option is curtailed."[99]

For the technologically advanced country, the advancing precision of its surveillance and targeting capabilities could drive escalation in a crisis by increasing counterforce incentives of a "splendid" first strike that could disarm an adversary of its nuclear weapons before it could launch them in retaliation. By creating greater vulnerability for the targeted state's nuclear and missile forces, the targeting state may be more confident that a disarming escalatory strike would be successful and limit the possibility for retaliation.[100] Once capabilities such as UAVs identify possible targets, other conventional capabilities (often with higher-resolution sensors) are then able to continue the mission of precisely locating, identifying, and potentially targeting for kinetic action. Whereas UAVs can be denied access to adversary airspace, satellites orbit far above adversary territory and are much harder to disrupt (but still possible, depending on technical capabilities). An increasingly valuable capability for targeting both conventional and nuclear mobile assets is synthetic aperture radar (SAR). Until

recently, this type of radar employed on most satellites could not image moving targets, but over the past two decades, advances in data-processing techniques have enabled SAR to both detect moving targets and determine their speed and direction of travel, making this conventional SA capability extremely valuable for tracking mobile targets and increasing incentives for preemptive action.[101]

Entanglement

Strategic SA can introduce escalatory risks along the entanglement pathway when parties to a crisis or conflict are unable to delineate between nuclear and conventional risks, thereby increasing the risk of miscalculation and unintended escalation. This can happen when conventional SA systems intentionally or unintentionally collect information on nuclear assets or when dual-use SA systems become military targets during a conventional conflict. Entanglement can also lead to escalation by convincing one or more countries in a crisis that their nuclear assets are at risk.

Research to date on entanglement has focused on several risks associated with the comingling of conventional and nuclear forces that could lead to escalation: (1) dual-use delivery systems that can be armed with nuclear and non-nuclear warheads; (2) the comingling of nuclear and non-nuclear forces and their support structures; and (3) non-nuclear threats to nuclear weapons and their associated C3I systems.[102] This definition is expansive but fails to account for the significance of the overall strategic SA ecosystem that is emerging, which introduces additional entanglement concerns associated with methods and systems meant solely to increase one's own SA (or obfuscate an adversary's SA). While these actions have not traditionally been viewed as particularly escalatory (as increased SA has been understood to increase strategic stability), the increased comingling of conventional and nuclear systems means improving SA as it relates to a conventional conflict could prompt either party to believe the conflict has entered a more dangerous phase, one in which the use of nuclear weapons (or an attempt to pre-empt their use) is possible.

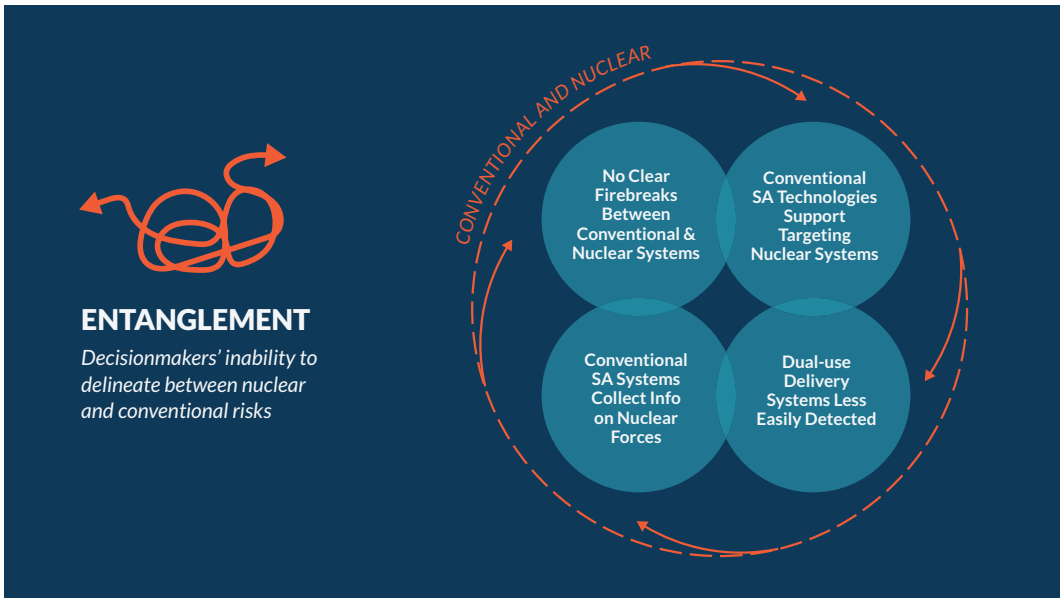
STRATEGIC SA ENTANGLEMENT THREATS

More specifically, there are four major reasons this entanglement in the strategic SA ecosystem could lead to escalation. These are:

1. The emerging strategic SA ecosystem does not have clear firebreaks between conventional and nuclear systems, including for strategic warning and communications;
2. Conventional SA technologies are increasingly able to support targeting of nuclear/strategic systems;
3. Conventional/dual-use delivery systems are less easily detected and have less warning, therefore creating a growing desire for pre-launch warning; and
4. In crisis or conflict, conventional targeting of conventional strategic SA-related assets, especially if linked to command and control (C2) or decisionmaking, may still raise strategic escalation risks.

These risks can be overlapping and are not mutually exclusive. Comingled nuclear and conventional systems run the risk of exacerbating any number of these scenarios, and decisionmakers may decide against employing capabilities to avoid misinterpretation. Increasingly, however, as competition between nuclear-armed states continues, these four aspects of the strategic SA environment can play a role in determining how conflicts escalate.

Figure 4.2



First, the emerging strategic SA ecosystem lacks physical firebreaks, or tripwires, between conventional and nuclear systems, including for strategic warning and communications that might counter or disrupt escalatory pressures. This is significant as the dual-use nature of such capabilities means attacks on a warning or communications capability for strictly conventional purposes could be misconstrued as an effort to "blind" the target before launching a nuclear strike.

A major component of the strategic warning infrastructure for the United States is the array of satellites that can provide warning of nuclear launches and detect nuclear detonations. Until the mid-1980s, early-warning satellites employed by the United States were used exclusively for detecting the launch of nuclear missiles.[103] Similarly, the Air Force Technical Applications Center (AFTAC), the U.S. military organization that historically focused almost entirely on following Soviet nuclear weapons development, used satellites designed exclusively to detect nuclear explosions in the atmosphere or space until the 1980s, after which it began piggybacking on satellites deployed for other purposes.[104] Since then, motivating factors such as cost and flexibility have prompted the move toward using the same platforms for conventional tasks as well. For example, the U.S. Space-Based Infrared System (SBIRS) is a constellation of integrated satellites that enables such varied missions as providing early missile warning, cueing missile defenses, delivering technical intelligence, and supporting SA.[105]

Over the course of a conventional conflict between the United States and an adversary with ASAT capabilities, the use of such capabilities against dual-use satellites that provide early-warning functions would threaten escalation, as intentions would be difficult to discern. For example, some Chinese experts have argued that during a hypothetical conventional war with the United States, China should consider taking action against U.S. early-warning satellites to ensure the efficacy of conventional missile strikes against regional targets, an action that could be misinterpreted as an attempt to undermine the U.S. capacity to intercept Chinese ICBMs launched against the U.S. homeland.[106] Even if China has no intention of launching ICBMs against the U.S. homeland in this scenario, the perception associated with disabling or destroying an early-warning satellite could be highly escalatory, as decisionmakers would have reduced strategic SA throughout the scenario.

The U.S. Air Force's 45th Space Wing supported United Launch Alliance's successful launch of the third Space Based Infrared Systems Geosynchronous Earth Orbit spacecraft aboard an Atlas V rocket from Launch Complex 41 here Jan. 20 at 7:42 p.m. ET.

United Launch Alliance

The second risk for entanglement in strategic SA concerns the ability of conventional SA capabilities to support the targeting of nuclear forces and their support systems. Whereas the traditional command, control, surveillance, and warning systems focused either on nuclear warning ("nuclear" strategic SA systems) or on providing intelligence to commanders about the conventional battlefield ("conventional" strategic SA systems), today's dual-use strategic SA capabilities may be tasked to conduct both missions. This blurring effect between the conventional and nuclear potentially creates nuclear missions for what were previously considered conventional capabilities. For example, the RQ-4 Global Hawk is intended "to support joint combatant forces in worldwide peacetime, contingency and wartime operations" against a range of high value targets.[107] As Keir Lieber and Daryl Press suggest, increasingly capable UAVs like the Global Hawk, with advanced stealth and sensor capabilities, may also be useful to track a small country's mobile missiles, be they nuclear or conventional.[108]

Another conventional SA capability that could improve targeting of nuclear systems is non-acoustic submarine detection, which could be used to track both an adversary's conventional-only attack submarines as well as nuclear-armed SSBNs. Using light-based imaging or magnetic detection instruments, detection efforts have the potential to expose the location of SSBNs—capabilities that derive strategic significance from their ability to covertly maintain a second-strike capability.[109] If these SSBNs were targeted during a crisis using such detection methods, the surveilled state may believe the sea leg of their nuclear deterrent was compromised, potentially creating unintentional escalation.

The Ohio-class ballistic missile submarine USS Pennsylvania (SSBN 735) transits the Hood Canal as the boat returns to its homeport at Naval Base Kitsap-Bangor, Wash., following a routine strategic deterrent patrol Dec. 27, 2017.

U.S. Navy photo by Mass Communication Specialist 1st Class Amanda R. Gray

Advances in conventional and dual-use delivery systems have precipitated the third risk of entanglement in strategic SA in which weapons like hypersonic and cruise missiles are less easily detected and validated with traditional missile warning systems, creating a desire for more precise and widespread warning systems and pre-launch surveillance, with implications for both conventional and strategic conflict. For example, hypersonic weapons (both hypersonic glide vehicles and hypersonic cruise missiles), long-range traditional cruise missiles, and other capabilities are designed to elude traditional U.S. early-warning systems (i.e., radars and satellites), reduce confidence in warning, and defeat U.S. missile defenses. Traditional ballistic missiles leave the atmosphere and follow an unpowered trajectory before reentering the atmosphere toward a predetermined target. Missile defense systems, including Ground-based Midcourse Defense, rely on an advanced network of land, sea, and space sensors as well as ground-based interceptors that work together to track and target potential threats.[110] Hypersonic weapons aim to challenge detection and defenses using their speed, maneuverability, and low-altitude flight trajectory.[111] To counter these new delivery systems, the United States may have to rely on conventional SA systems, including systems that are more visible or dual use, to complete strategic missions and supplement strategic surveillance warning.

In addition, missile defense capabilities are viewed by some as having potential dual-use purposes. For example, China strenuously objects to the U.S. deployment of Terminal High-Altitude Area Defense (THAAD) missile batteries and their accompanying radar systems in South Korea. In this context, THAAD is primarily a missile defense system with a stated goal of intercepting North Korean short-range ballistic missiles using interceptors with a range of 200km.[112] However, its deployment has alarmed Beijing. Public statements suggest the Chinese government is concerned about potential uses of the AN/TPY-2 radar deployed with THAAD, fearing it could be used to gather information about its missile tests (both conventional and nuclear-capable) and other military operations, thus weakening the credibility of China's nuclear deterrent.[113] If an adversary were to feel threatened in a crisis and target such systems, would such an attack be considered conventional or strategic in intent and implication?

The final risk associated with entanglement is that of conventional targeting of conventional strategic SA-related assets that can nevertheless cause strategic escalation. As strategic SA systems become more networked and dual use, the threat of conventional attacks on them become more escalatory because states employing the capability are unable to determine if the attack is intended to degrade their conventional war-fighting capacity or their nuclear capacity. This escalatory threat is heightened if the conventional strategic SA is associated with C2 or decisionmaking activities. Examples of such threats include the networks of satellites employed by various states for dual-use purposes. The United States, for instance, has never fielded communication satellites used exclusively for nuclear operations.[114] While these satellites may have previously been perceived as impervious to adversary disruption, advances in ASAT capabilities may render these systems vulnerable. Satellite jamming, a conventional electronic attack that interferes with communications travelling to and from a satellite, runs the risk of leaving a targeted state strategically blinded, which could lead to "misinterpreted warning."[115] Although jamming ASAT capabilities have temporary effects (as the signal can be turned off and thereby restore adversary communications), states have strong incentives to target C2 warning and surveillance systems early in a crisis in order to ensure conventional dominance, intentionally or unintentionally threatening nuclear-related systems as well.

In addition to the space domain, computer networks that provide strategic SA can be dual use and are at risk of this type of escalatory threat. By employing an invasive cyber capability to collect information on an adversary's systems, actions, or intent, the very nature of that collection could trigger an escalatory response. For example, developments in cyberwarfare and electronic warfare have the potential to threaten previously secure strategic SA capabilities: Chinese experts believe the U.S. government is exploring the option of using cyber weapons to undermine adversary C2 during a crisis to prevent missile launches.[116] Even if the intent is not to sabotage nuclear systems but rather collect information (on either conventional or nuclear capabilities), the perception is what matters, and collecting information could prompt the target state to escalate a crisis if it fears its nuclear deterrent is compromised.

STRATEGIC SA AND ENTANGLEMENT: NO LOOKING BACK

This new, increasingly complex, and integrated technology ecosystem provides clear benefits for both conventional and nuclear systems while simultaneously complicating the ability of decisionmakers to delineate between these dual-use purposes during a crisis or conflict. For the United States, prosecuting any type of conventional war without the extensive use of such capabilities and the information dominance they provide is unimaginable. This combined ecosystem may increase the risk of miscalculation and unintended escalation, as nuclear-armed adversaries face difficulty navigating crises while holding the risk of nuclear escalation at bay. In this way, the strategic SA ecosystem not only introduces new entanglement challenges, but these escalatory risks may also be less easily mitigated by strategies to "disentangle" or separate these capabilities given their essential and multipurposed roles early in crisis. These roles may even prove "indivisible."

Moving forward, the highly networked nature of conventional systems, as well as the dual-capable nature of many of them, may increase the potential for conflict to bleed from the conventional into the nuclear realm. Technical firebreaks have all but disappeared between many systems, opening the possibility that actions taken to gain information on conventional assets will be easily confused with more escalatory intrusions of nuclear-related systems. Historically, the conceptual validity of the "stability-instability paradox" was reinforced by distinct and stratified conventional and

strategic systems of warfare that amplified the division between strategic and conventional war. In a world in which these systems are increasingly dual use over the long term, the durability of that reassuring theoretical construct may be called into question, and new tools will be needed to replace the escalatory firebreaks that differentiated nuclear and conventional warning and surveillance systems that existed in the past.

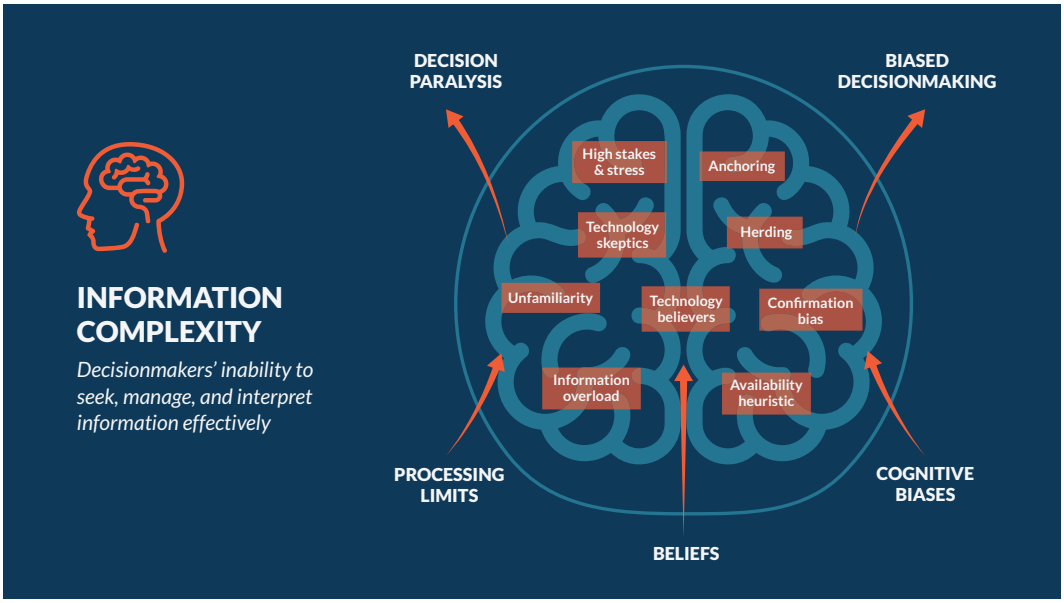
Information Complexity

Emerging technologies for strategic SA have the potential to fundamentally transform the information domain and, if used effectively, to help decisionmakers manage crises more effectively with lower levels of risk. An important characteristic of the emerging strategic SA environment is the large volumes of data and information that is collected. The U.S. Air Force has defined this new information environment by four "Vs"—greater volume (collection of magnitudes more data points), greater velocity (the volume of data is acquired at extreme speeds), variety (numerous formats of information from diverse sources), and veracity (the volume, velocity, and variety of data includes a significant amount of noise and irrelevant data).[117] In a similar vein, the U.S. Navy has reported being overwhelmed by the floods of data generated from its existing information gathering systems. According to a RAND Corporation study, the amount of data being collected by the U.S. Navy increased at an exponential rate between 2000 and 2015.[118] Thus, information complexity describes the challenges decisionmakers' encounter as they seek, manage, and interpret information in this new environment.

Information complexity contributes to two potentially escalatory decisionmaking scenarios:

- **Decision paralysis:** the inability to make or finalize a decision in the time frame necessary, due to information overload or information shortfalls; and
- **Biased decisionmaking:** the excessive intrusion of belief or cognitive biases into the decisionmaking process in ways that diminish or discredit objective data and distort decisional outcomes.

Figure 4.3



These faulty decisionmaking outcomes result from the existence and interplay of several conditions, including cognitive processing limits, unacknowledged belief or value systems regarding information sources, and cognitive biases. The interaction of these factors may work to potentially impair effective crisis management and increase escalation risks. Processing limits, poor information management, and cognitive biases are longstanding risks in crisis management. However, the combination of increasingly complex information sources, unfamiliar technologies, and the high-stakes/high-stress nature of nuclear crises suggests that the escalatory risks associated with information complexity may be a growing concern.

DECISION PARALYSIS

Information overload occurs when the volume of input to a system exceeds its processing capacity.[119] Critically, decisionmakers have limited cognitive processing capacity.[120] Emerging SA technology potentially can provide more accurate, detailed, and timely information that can help reduce ambiguity and differentiate credible information from the uncertain during a nuclear crisis. But this is only possible if the information can be organized, communicated, and absorbed effectively.[121] In addition to the quantity of information, the specific characteristics and quality of information can influence the degree of information overload as well.[122] Indeed, at the individual level, the development of new communication and information technologies has been recognized as an important factor in information overload.[123] Thus, in the emerging strategic SA ecosystem—where the volume, velocity, and variety of information have increased considerably and the veracity of information may at times be unclear—information overload is likely to become a more pronounced concern for decisionmakers.

For instance, distributed sensing platforms such as cubesats and swarmed unmanned vehicles may produce new streams of information to collectors and policymakers, complementing traditional data sources and providing needed confirmations of important observations. Miniaturization and improvements in networking are enabling the wide deployment of formerly limited capabilities, such as aerial full-motion video, and the exploitation of open sources, such as commercial satellite imagery and geographic information systems (GIS) data, all of which further increases information loads.[124] Combined with the data-mining capacity of cyber surveillance and the pattern recognition capacity of AI, the volume of information potentially available to enhance SA in a crisis is enormous. But if multiple data streams emerge with varying or divergent levels of confidence, decisionmakers may be overwhelmed with data or unable to differentiate data quality, especially if the provenance and validity of information cannot be demonstrably verified.

U.S. Soldiers assigned to the 7th Special Forces Group conduct urban warfare training during Emerald Warrior 17 at Hurlburt Field, Fla., March 7, 2017.

U.S. Air Force photo by Tech. Sgt. Barry Loo

The research is clear that increased information volume from SA technologies does not necessarily produce better decisionmaking. Indeed, when supply of information exceeds information-processing capacity, there is "widespread consensus" that performance is negatively affected.[125] At the individual level, information overload is linked with information anxiety and the inability to use relevant information to make a decision.[126] In the consumer context, individuals require more time to analyze information and reach a decision.[127] Similar experiments identify a range of cognitive and psychological effects whereby subjects tend to discard complex or conflicting information, settle for suboptimal conclusions to save time, and experience high levels of stress and other negative psychological effects.[128]

A recent study that measured performance of simulated C2 tasks with varying information volume and reliability found that increased volumes of task-relevant information did not improve task performance and led study participants to self-report reduced SA and interpersonal trust in their team members.[129] Upon encountering an overload of information with limited processing capacity, decisionmakers may face an impasse and fail to reach or communicate a decision. The failure to reach a decision advantages an adversary and could potentially result in further escalation. In a crisis, failure to reach a decision is a decision.

BIASED DECISIONMAKING

Information overload and technology uncertainty or unfamiliarity also increase the influence of bias in decisionmaking. Overvaluing or undervaluing certain types and sources of information form part of the mental heuristics, or shortcuts, decisionmakers will use to discount or replace information sources in ways that are consistent with their beliefs.[130] Many decisionmakers have potent belief biases—both positive and negative—about the value and reliability of information and decision-support technologies.[131] This dynamic is prominently discussed in the context of AI, where the relative merits, reliability, and applicability of AI tools have been hotly debated and on which many policymakers have strongly-held views. This tension is best encapsulated by former Google CEO Eric Schmidt's 2018 statement, "[the] DoD does not have an innovation problem; it has an innovation adoption problem."[132] Decisionmakers tend to fall into one of two camps: the technology skeptics and the technology true believers.

The skeptics respond to new technologies with trepidation due to unfamiliarity and mistrust, which may make them discard information generated from emerging SA technology or fail to acquire enough information in the first place. This is especially acute with issues regarding the displacement of human decisionmaking with autonomous systems, machine learning, and AI. AI derives some of its unique advantages from being able to recognize patterns that human analysts cannot, but if the indicators that an AI system cites do not match a decisionmaker's idea of relevant indicators, they may dismiss it. AI systems may be seen as a "black box," making important decisions when few people outside of analytics teams, data science labs, and technology centers can fully understand how.

The skeptics respond to new technologies with trepidation due to unfamiliarity and mistrust, which may make them discard information generated from emerging SA technology or fail to acquire enough information in the first place.

Moreover, some technology resistance comes from the concern that decisionmakers will be

"black boxed"—forced to make decisions that must be publicly defensible or explainable based on information that is not.[133] AI is a principle source of concern in this regard, despite the fact that AI is expected to be particularly useful in collection.[134] Experts remain wary of relying on AI because AI systems cannot always explain how conclusions were derived and because the veracity of information can be difficult to judge. Senior decisionmakers are typically held accountable to the public and the institutions they lead for the decisions they make and are expected to explain and justify those decisions publicly to both domestic and international audiences.[135] However, this is difficult if the information on which the decision rests is not sharable or explainable. Moreover, when policymakers are bereft of a baseline understanding or grasp of AI, they will be unable to determine its practical limits and potential benefits.[136]

Reluctance to accept technology also stems from concerns about the vulnerability of technology to tampering or manipulation. Advances in autonomy and machine learning mean that a much broader range of physical systems are now susceptible to cyberattacks, including hacking, spoofing, and data poisoning. Similarly, machine learning-generated deepfakes (i.e., audio or video manipulation) have added a novel and potentially more sinister twist to the risk of miscalculation, misperception, and inadvertent escalation that originates in cyberspace but has a very real impact in the physical world.[137] Further, unmanned aerial systems may also fail due to multiple factors, including operator error, improper maintenance, loss of communication, equipment failure, and weather, among others. As the system matures, some causes of failure are largely mitigated (e.g., equipment failure), while other causes tend to persist (e.g., the risk of operator error).[138] Such qualms may make policymakers almost too cautious when deciding to deploy unmanned systems amid a crisis, creating information gaps and potentially heightening the risk that the United States and its allies could be surprised and disadvantaged during a conflict.

Advances in autonomy and machine learning mean that a much broader range of physical systems are now susceptible to cyberattacks, including hacking, spoofing, and data poisoning.

In stark contrast, risky belief biases run equally strong among the technology "true believers." These technology advocates are highly confident in given technologies and place considerable faith in the information they provide. In business psychology, this is known as the "technology effect," and research in this area suggests an implicit association between technology and success. Signals of high performance trigger the effect, and the effect is more likely when the technology invoked is unfamiliar.[139] One of the potential risks exacerbated by the complexity of data collection and analysis is the potential for analysts to operate on the faith that their systems yield appropriate insights. While SA technology has advanced to provide higher levels of detail and quality, this may contribute to a heightened degree of confidence in the information collected. However, the complexity of the technology hardware and software (e.g., distributed sensor networks with complicated information processing systems or AI systems with unexplainable algorithms) can make independent verification of the assessments obtained from these systems nearly impossible. The level of sophistication of emerging SA technology may lead to undue confidence in the assessments with no means for an independent cross-check.

Both technology skeptics and technology true believers risk engaging in biased decisionmaking by either accepting or rejecting information sets based on heuristics that seek to manage informational

The level of sophistication of emerging SA technology may lead to undue confidence in the assessments with no means for an independent cross-check.

complexity, both of which can exacerbate escalatory risks. If policymakers exhibit excessive caution from low belief in emerging SA technologies, they may reject or fail to obtain available information necessary for critically evaluating the positives and negatives of a preferred course of action and other alternatives. If an information search is perfunctory and incomplete, it fails to obtain several important pieces of information that may be crucial to defuse a crisis. While restraint is often perceived to be good, if it leaves policymakers in the dark, the opposite could also be true.[140] Although information dominance does not guarantee stability, its opposite—information inadequacy—may also serve to be an impediment to strategic stability.

RELIANCE ON COGNITIVE BIASES

Belief systems regarding the role and utility of technology are by no means the only way biased decisionmaking can emerge in crisis scenarios. When problems include an unclear environment, an overload of data, lack of confidence in data sources, and lack of time for rigorous assessment of sources and validity, ambiguity may abet instinct and permit intuition to steer analysis. Potentially, the greater the ambiguity, the greater the likelihood that decisions will be driven by preconceptions.[141] Preconceptions could become a coping mechanism to simplify reality and mitigate information complexity. Cognitive bias—a challenge for all decisionmakers—may be exacerbated in the emerging strategic SA ecosystem where unfamiliar technologies or manifold sources of information are more prominent. In particular, perceptions of historical lessons from past crises that might have little relevance could also have outsized influence on decisionmakers who seek to ground decisionmaking in precedent and experience.[142]

When problems include an unclear environment, an overload of data, lack of confidence in data sources, and lack of time for rigorous assessment of sources and validity, ambiguity may abet instinct and permit intuition to steer analysis.

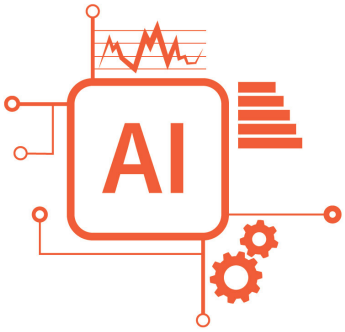
While a range of cognitive biases can be exacerbated by information complexity in crisis decision-making, overconfidence bias, confirmation bias, anchoring, and availability heuristic seem particularly challenging in these settings.[143] In the case of anchoring, psychologists have found that people tend to rely too heavily on the very first piece of information they learn, while discounting later information.[144] When it comes to emerging technology for SA, without a streamlined approach to deconflict a multiplicity of sources and with preconceived skepticism or unfamiliarity, decisionmakers may overvalue early sources rather than pursuing further options. Equally significant is the intrusion of confirmation bias—the tendency to search for, interpret, favor, and recall information in a way that confirms or strengthens one's prior personal beliefs or hypotheses. As described earlier, if a decisionmaker has low belief in an emerging SA technology, they may value evidence that supports this belief disproportionately to information that does not. This is particularly the case with AI: people are predisposed to view conclusions produced by humans as more transparent and explainable than those produced by AI-based methods but consistently overestimate the ability of humans to

explain their own deliberative processes.[145] Finally, the availability heuristic is a mental shortcut that relies on immediate examples that come to a person's mind when evaluating a specific topic, concept, method, or decision. The availability heuristic operates on the notion that if something can be recalled, it must be important, or at least more important than alternative information which is not as readily recalled.[146] Subsequently, under the availability heuristic, people tend to heavily weigh their judgments toward more recent or more memorable information and experiences, making new opinions biased toward that which can be more easily recalled.

One significant problem inherent to the aggregation of different information sources is the possibility that coincidental events will be misinterpreted. Escalated tensions over an individual issue could cause other, innocent actions to be perceived as aggressive or otherwise contribute to confirmation bias. Paul Bracken explores one historical example in detail: the connection between the Hungarian Revolution and Suez Crisis in 1956. In this case, unrelated events—Soviet fleet exercises involving transit through the Dardanelles, a British jet crash in Syria, and erroneous reports of Soviet troops movements by radar operators—coincided with heightened tensions over both incidents to give the impression of imminent Soviet intervention in Egypt.[147] In today's technology environment, such biases can be compounded by the integration of information streams and by efforts to supply information more directly and more quickly to policymakers via emerging strategic SA technology.[148]

NAVIGATING INFORMATION COMPLEXITY

New research is examining promising ways in which training might reduce or mitigate the negative impact of cognitive biases and pre-held beliefs. Training may effectively debias decisionmakers over the long term.[149] In fact, experiments by Morewedge et al. (2015) find that interactive computer games and instructional videos can result in long-term debiasing at a general level. In a series of experiments, training with interactive computer games that provided players with personalized feedback, mitigating strategies, and practice reduced six cognitive biases by more than 30 percent immediately and by more than 20 percent as much as three months later. The biases reduced were anchoring, bias blind spot, confirmation bias, fundamental attribution error, projection bias, and representativeness.[150] The medical field is also recognizing the risks associated with decisional bias and seeking new training to reduce its negative effects on patient outcomes.[151] Research in medicinal debiasing emphasizes that experience in the field does not guarantee expertise, and debiasing for emerging technologies at more senior levels is sorely needed, since expert biases may run counter to next-generation scholars.[152] Fields as disparate as medicine and business are emphasizing the risks posed by biased decisionmaking and are developing tools to reduce them. Ultimately, their conclusions will prove equally relevant in national security crises between nuclear-armed states, where emerging technologies in a novel information space will engender problematic decisionmaking unless bias mitigation occurs.



5 | Tabletop Exercise Takeaways

An analysis of strategic SA capabilities according to the attributes and risk factors they could introduce in a crisis suggests some of the ways these technologies could pose escalatory risk, complicate decisionmaking, and challenge traditional notions of information dominance in the strategic SA ecosystem. And yet, real-world case studies or other experiential sources of information to evaluate these assessments are highly limited or overly dated. To evaluate some of the risk assessments identified in research and explore the decisionmaking process of policymakers and technical experts in the throes of crises under a nuclear shadow, the Project on Nuclear Issues (PONI) developed and conducted a series of tabletop exercises on two fictitious regional scenarios. These exercises provided insight regarding both the decisionmaking calculus involved in deploying emerging SA technologies and how their use could potentially impact strategic stability.

Conducted eight times over the last year, with nearly 150 people overall, the tabletop exercises involved a wide range of participants, from senior policy experts with significant government decisionmaking experience to several next-generation nuclear scholars, researchers, and operators. The scenarios sought to inform the policy implications of the theoretical analysis, understand how sensitive U.S. decisionmakers might be to the risks associated with these technologies, and draw conclusions on potential ways to improve crisis decisionmaking and escalation management. The tabletops were not designed to emphasize highly uniform and consistent variables and generate replicable, quantifiable data results but rather to inform a discussion and serve as a learning experience for both participants and observers. What this series of tabletop exercises offers is not concrete facts or indisputable knowledge but a deeper understanding of the human aspect of decisionmaking in nuclear crises.[153] This process provided unique insights irretrievable through traditional academic approaches, raised awareness about strategic SA risk and complexity among both technical and policy participants, and highlighted areas where extant high levels of escalatory anxiety may complicate and even increase escalatory risk—a set of outcomes not fully anticipated in the research phase.

Using two different scenarios across eight different exercises, the study team examined the variation in potential decisionmaker reactions according to the level of intensity of the crisis and different military capabilities, both conventional and nuclear.

Using two different scenarios across eight different exercises, the study team examined the variation in potential decisionmaker

reactions according to the level of intensity of the crisis and different military capabilities, both conventional and nuclear. The China scenario represented a potential "near-peer" in a comparatively early crisis, and the North Korea scenario represented a far more asymmetrical adversary in a more advanced crisis where the initial stages of military conflict are already underway. In both cases, the scenarios took place approximately five years in the future under geopolitical circumstances roughly similar to the present. The SA capabilities discussed and evaluated were all deemed to be technically feasible in the five-year time frame and operationally available for the purposes of the exercise.

Figure 5.1 List of Tabletop Exercises Conducted

LOCATION	DATE	SCENARIO
1. University of California, Berkeley	*February 4, 2019*	*China*
2. Lawrence Livermore National Laboratory	*February 6, 2019*	*China*
3. National Defense University	*April 17, 2019*	*China*
4. CSIS Nuclear Scholars	*June 26, 2019*	*China*
4. CSIS Nuclear Scholars	*June 27, 2019*	*North Korea*
6. Kings Bay Naval Base	*October 17 ,2019*	*China*
6. Kings Bay Naval Base	*October 17 ,2019*	*North Korea*
8. CSIS Senior Experts	*October 28, 2019*	*North Korea*

The first scenario, "Blind Spot," presented a political crisis in the Taiwan Straits precipitated by Chinese escalation in the region and focused on competition between near-peer adversaries. The scenario takes place in 2024 at a time of increasing Chinese pressure to assert regional dominance primarily through economic and grey zone tactics, with reunification with Taiwan an increasing priority. Following a close-approach incident between the Chinese and Taiwanese navies in the Taiwan Strait, China demands the withdrawal of Taiwan's naval assets from the strait, accelerates the timeline for its yearly live-fire exercise, and extends its air defense identification zone (ADIZ) beyond the first island chain while dialing up its rhetoric regarding reunification. Twelve hours before the simulation exercise, U.S. Navy ships near Taiwan have reported significant satellite navigation errors preventing them from conducting regular operations. Several U.S. remote sensing satellites, which provide critical intelligence, surveillance, and reconnaissance (ISR) of Taiwan and the surrounding region, are no longer providing imagery. Facing a growing regional outcry, participants in the exercise are given presidential guidance and objectives to shape their crisis decisions, such as protecting U.S. forces and vital interests in the region, limiting China's expanding influence, and assuring U.S. allies of its commitment to defend their security while avoiding escalation.

The second scenario, "Risky Business," explores the exacerbation of an inter-Korean crisis on the Korean Peninsula. In this scenario, the U.S.-North Korea relationship has reverted to an uneasy deterrent relationship following the breakdown of denuclearization talks, the return of a conservative coalition government in South Korea, and continued economic decline in North Korea. The crisis unfolds when North Korea attacks Baengnyeong Island following a shipping vessel dispute, takes 50 South Korean marines hostage, and issues a series of demands for economic relief and political accommodation. When immediate demands are not met, North Korean forces cross the demilitarized zone (DMZ) on the far-

Republic of Korea Air Force F-16 Fighting Falcon aircraft pilots prepare to take off during Red Flag-Alaska 15-1 at Eielson Air Force Base, Alaska, Oct. 9, 2014.

DoD photo by Tech. Sgt. Joseph Swafford Jr., U.S. Air Force/Released

east side of the peninsula and establish a position on a ridge 20 kilometers into South Korean territory. Presidential guidance includes insistence on restoration of the status quo ante while preventing North Korea's use of nuclear or other weapons of mass destruction against the United States or its allies and avoiding wide-scale conventional war on the peninsula.

DESIGN AND EXECUTION OF THE EXERCISE

In each exercise, participants were split into two groups—a technology team and a policy team. Representing the technical collection communities of the U.S. Intelligence Community and Department of Defense, the technology groups evaluated the utility of a set of strategic SA options (a "collection plan"), which they then briefed to a group of policy decisionmakers for approval. The technology team was tasked with developing a series of options (capabilities and targets) to improve U.S. SA (a "collection plan") and then present the plan to the policy team.

The policy group represented a high-level group of interagency decisionmakers (a notional Deputies Committee) charged with providing advice to the president and implementing presidential guidance. In some of the tabletop exercises, technical groups met contemporaneously with the policy groups; at other times, in order to reduce the time and administrative burden of the exercise, the technical group met virtually in advance to come up with the proposed collection plan which was then briefed to the policy group during the in-person exercise. The policy group was tasked with evaluating the crisis and associated priorities, interpreting presidential guidance, and approving or disapproving the collection plan following discussion of each of the proposed actions. In addition, the policy group would provide additional guidance and limitations, or "guardrails," designed to limit the escalatory risks they identified with some of the approved options. Ultimately, the policy team was responsible for deciding whether to approve each option in the collection plan developed by the technology team. During the collection plan approval process, the technology team contributed to the discussion and answered questions about the collection options. However, the technology team was not allowed to vote to approve/disapprove specific options. Figure 5.2 offers a top line summary of the types of technologies that were offered to

Figure 5.2 Voting Results Across Exercises

VOTING TABLE

DOMAIN	CAPABILITY	APPROVALS OUT OF TIMES OFFERED, CHINA	APPROVALS OUT OF TIMES OFFERED, NORTH KOREA	GUARDRAILS
SPACE	Small Sat	6 out of 8	6 out of 6	*Deployment must be accompanied with diplomatic message; approved with order of preference for use of smallsats to be firstly to monitor maritime forces, then conventional ground forces, and lastly nuclear forces*
AIR	Manned Stealth Aircraft	2 out of 5	1 out of 3	*Approved only for missions that did not violate Chinese airspace*
	UAV	15 out of 25	16 out of 25	*National territory off-limits; Launch facilities only; Only deployed in allied airspace; safeguard this asset for eventual future use*
				In allied littorals only if sufficient information was exchanged with the allies and if the United States properly signaled to the adversary that the swarm was unarmed
				Approved only for missions that did not violate adversarial airspace
				Approved only for missions that did not violate adversarial airspace
SEA	UUV	9 out of 15	1 out of 3	*Deploy only in the contested areas outside of adversary's territorial waters*
				Only to be deployed at chokepoints located within international waters
	Unmanned Surface Vehicles	3 out of 6	1 out of 3	*Only to international and contested waters*
CYBER	Zero Day Exploit	4 out of 7	3 out of 3	*Cyber must be overt and reversible; purely passive collection amd not offesnive or degradatory; safeguard this asset for eventual future use*
	AI Analysis Application	5 out of 6	3 out of 3	*Operators must have established high confidence in this technology prior to deployment; AI must be tested pre-crisis; Don't share methods with allies, just the results*
LAND/ DIRECT PLACEMENT	Compact multi-sensor devices	1 out of 4	2 out of 2	*Allied SOF insertion; inform ally before deploying*

decisionmakers, and how often they chose to utilize them to close critical information gaps. In addition, this chart includes examples of the types of guardrails/conditions that the policy groups levied for using the capabilities, if approved at all.

Analysis

TECH VERSUS POLICY: TWO ROADS DIVERGED

Technology groups were consistently surprised by policy decisionmaking they believed to be "irrational" or unduly conservative given the state of related technology, its broad acceptance and utility in conventional conflicts, and the value they believed it could provide. Technology groups consistently underestimated the level of caution that policymakers might bring to a crisis between nuclear-armed adversaries.

By contrast, policymakers were highly attuned to the escalatory risk associated with intrusive technologies, often weighing their concerns about the potential provocation risks to be more important than the SA benefit that capabilities may provide. Even when such capabilities were approved, policymakers routinely placed guardrails—geographic, target-based, or other—to limit the use of intrusive technologies. Generally, policy participants were so concerned about using any collection options that seemed to be intrusive that they were reluctant to intrude on sovereign territory, waters, or airspace. Such caution was evident even in the North Korea scenario, during which the crisis was presented as severe, the informational benefits potentially significant, and the U.S. asymmetric advantages quite substantial.

INTRUSIVENESS AND SOVEREIGNTY

U.S. policymakers placed high value on internationally recognized borders and Western legal interpretations of "sovereignty." In other words, crossings of internationally recognized "sovereign" borders were interpreted as legally provocative and not just escalatory from a crisis management perspective. When confronted with adversary territorial claims (such as an expanded and enforced ADIZ), policymakers had fewer concerns with placing collection assets in these disputed areas but remained highly cautious and preferred overt modes of collection that could be used for signaling purposes as well as information collection. This remained true even when the adversary in the scenario was engaging in aggressive enforcement of the expanded claim (as in harassing Taiwanese or other ships' aircraft or in the case of North Korean forces establishing de facto control of the island). In these cases, however, policy groups focused on the signaling value of these collection platforms as much, and sometimes more, than their information collection value. Covert or stealthy intrusive capabilities were generally met with skepticism and concern that the risks of escalation by surprise and misunderstanding outweighed the benefits of secrecy.

DOMAIN-BASED PERCEPTION AND MISPERCEPTION

While perceived thresholds associated with sovereignty were highly valued by policymakers, they were not equally valued in all domains. Assets in the air domain were consistently seen as riskier and requiring higher guardrails than those in maritime or cyber domains. Sometimes the use of air-based assets was met with even more skepticism than use of capabilities that required covert emplacement within adversary territory. Some of this caution stemmed from the worry that escalatory risks associated with discovery of an air-based collection capability by the adversary could be provocative but also that the public destruction or shoot down of an air asset could force the United States into an escalatory response. Violating adversary airspace was a noteworthy concern: UAVs were deployed at

surprisingly similar levels across both scenarios, being approved in the China scenario approximately 60 percent of the time and in the North Korea scenario 64 percent of the time. All approvals were conditioned upon extensive use of guardrails to limit the territory in which the assets could be used.

> *While perceived thresholds associated with sovereignty were highly valued by policymakers, they were not equally valued in all domains. Assets in the air domain were consistently seen as riskier and requiring higher guardrails than those in maritime or cyber domains.*

Relatedly, policy players also frequently discounted the value and efficacy of stealth. They accepted it might make it easier to avoid loss but not to avoid detection, and therefore stealth on an air asset generally did not make the asset more likely to be deployed. Policy groups also engaged in robust (and sometimes counterintuitive) debates on the escalatory risks associated with manned versus unmanned aircraft. Technical groups almost always discouraged manned aircraft options for collection, even with advanced stealth, given almost all collection needs could be met with unmanned aircraft at lower operational risk. At times, this disagreement reflected the policy teams' unwillingness to differentiate intelligence collection and signaling, such as when some groups sought to deploy manned aircraft as a signal of determined resolve. In other cases, policy groups sought to raise the escalatory stakes for the adversary while reducing the risk of surprise or misunderstanding as to U.S. intentions by preferring overt and, in some cases, manned aircraft over unmanned and highly vulnerable aircraft like HALE UAVs. Overall, manned aircraft were approved only 40 percent of the time in the China scenario and not at all in the North Korea scenario; these choices were guided almost entirely by policymakers' perceptions of escalation management and signaling rather than informational demands or benefits.

Discussions along these lines became much more pronounced following the Iranian shoot down of a U.S. Global Hawk.[154] The session held after the Global Hawk shoot down involved an extensive discussion of the risk of shoot down of unmanned assets as too easy or appealing for China. That group determined that it was essential to assert U.S. willingness to put manned, non-stealthy assets into the contested area (but not over internationally recognized Chinese territory) before using unmanned assets and that clear deterrence-oriented, declaratory statements are needed regarding the targeting of surveillance assets. This was strongly considered as a means of rejecting Chinese claims of an expanded ADIZ while simultaneously collecting information in the China scenario. In many ways, these decisions may have represented "recency bias" in action, given proximity to the Iranian shootdown. In the North Korea scenario, policy groups remained reluctant to fly unmanned platforms over DPRK territory given the shoot down risk, and only authorized their use over the ROK or international waters or territories. Even in cases where the UAV platforms were approved, approvals were contentious and involved longer debates among participants than other aspects of the collection plan.

TWO IF BY SEA

Sea-based assets, both surface and subsurface, generally receive similar guardrails, but policymakers showed greater willingness both to risk these assets, in terms of discovery and loss, and see them as either more easily hidden (subsurface) or somewhat less provocative. Overall, unmanned underwater

The Navy's most technologically advanced surface ship USS Zumwalt (DDG 1000) steams in formation with USS Independence (LCS 2) and USS Bunker Hill (CG 52) on the final leg of her three-month journey to her new homeport in San Diego.

U.S. Navy Combat Camera photo by Petty Officer 1st Class Ace Rheaume/Released

vehicles (UUVs) were approved 60 percent of the time in the China scenario and one out of three times during the North Korea scenario—ratios roughly similar to the UAV approvals. However, the discrepancy is clear when more detailed options are considered. For example, static UUV nets deployed at key choke points were approved all four of the times offered in the China scenario and three of four times in the North Korea scenario. On the other hand, the more intrusive autonomous UUVs with advanced sensors that would provide far more actionable information were approved only 33 percent of the time in both scenarios.

During a discussion after the China exercise, one participant suggested that perhaps they had regarded naval assets as less escalatory because the crisis had begun in the naval domain and increased naval surveillance therefore seemed proportional. However, the deployment of aerial assets overall was consistently perceived as riskier than the use of underwater assets. The policy team often argued that underwater assets gave leeway for plausible deniability and the loss of an asset was less likely to prompt a public response or go viral on social media the way a more visible shootdown of an air asset might. For instance, should an adversary sink a U.S. underwater asset, it would be more difficult for an adversary to retrieve that asset, thus protecting U.S. technology from falling into adversary hands and allowing the United States the option to deny involvement. At least implicitly, the comparatively more public and visible nature of targeting and destroying an air asset in ways that could "force the hands" of policymakers seemed to weigh heavily on policy groups in ways that similar capabilities and sensors did not when used in the maritime domain.

While of little signaling value, subsurface capabilities did risk surprising an adversary, which could have difficulty distinguishing between armed and unarmed capabilities. Hence policy groups generally

rejected placing such collection platforms in proximity to sensitive targets. The utility of surface vessels as collection platforms were evaluated largely independent of their informational value; instead, approval decisions largely depended on whether a group weighed positive signaling benefits more than the risk of attack or loss.

In sum, policy groups remained very cautious with any intrusions into an adversary's airspace or territorial waters and in all cases approved these collection capabilities only with clear guardrails denying approval to enter sovereign territory, airspace, or waters and generally adjudicated the use of these platforms according to how they perceived their value in shaping the crisis overall.

SPACE AND CYBERSPACE

Even supplemental space assets raised interesting domain and sovereignty questions. What constitutes sovereign airspace? What about capabilities such as pseudosatellites or smallsats that are deployed from aircraft or exist in the region between outer space and airspace?[155] Smallsats represented a consistent point of divergence between technology and policy groups, particularly in the China scenario, which involved Chinese dazzling of U.S. naval navigational assets as part of the initial crisis. Tech groups consistently recommended the deployment of smallsats as providing targeted coverage and vital redundancy with relative safety. Policy groups were far more skeptical and sometimes dismissive, questioning the additional value-added to existing space systems, fearing additional targeting and disablement of vulnerable systems and expressing concern about how the launching and deployment of the constellation would be seen and perceived by the adversary during the crisis. Concerns were often assuaged with a back and forth between policy and tech teams. Thus, despite trepidation, co-orbital reconnaissance small satellites were approved in the China scenario 50 percent of the time, and smallsat constellations were approved 75 percent of the time. Policy teams playing the North Korea scenario approved these capabilities every single time they were offered.

Pseudosatellites, which are multi-payload, high-altitude air vehicles or airships able to maintain a fixed position over a single area of interest for extended periods of time, were initially met with skepticism from the policy groups. While tech groups saw the platform as providing persistent surveillance with impressive sensor capacity at safer distances, policy groups focused on the challenges of the high visibility deployment, concerns about intrusions into national airspace even at very high altitude, and vulnerability to attack and shootdown, among other concerns. After dialogue between the groups, voting patterns demonstrate greater trust in the capabilities—pseudosatellites were approved three out of three times offered in the China scenario and two out of three times for North Korea.

Cyberspace is one area where groups tended to diverge, with some participants treating cyberspace as highly intrusive and escalatory. Such participants were particularly concerned with any action that appeared to target adversary C2 and decisionmaking, typically out of fear that such action could escalate the crisis. In the China scenario, cyber espionage was only approved 57 percent of the time, as participants expressed wariness of inciting aggression. Others felt that it was less escalatory ("states do cyber intrusions all the time and it doesn't start wars"). Cyber espionage was approved every time it was offered on a North Korean collection plan. Several participants voiced the perspective that aggressive moves made by North Korea indicated a resumption of hostilities, and much of the discussion around capabilities focused not on if they should be deployed but rather when during the unfolding crisis they would be most effective. Accordingly, even though cyber espionage capabilities were approved for all missions, policy participants voiced concerns that the zero-day

> *Policymakers routinely expressed concerns about anything that appeared to target C2 assets, especially in the cyber domain.*

vulnerabilities were so valuable that it may be prudent to hold them for when they would have the most impact in the event of a military conflict (e.g., targeting North Korean leadership, tracking nuclear weapon deployment). In cyber-related options, discussion turned more to targets than to domain as areas of concern or potential constraints, but isolating targets in ways that would be demonstrable or transparent (and therefore presumably less escalatory) was very difficult.

Policymakers routinely expressed concerns about anything that appeared to target C2 assets, especially in the cyber domain. Groups could not articulate effective ways to differentiate between nuclear and conventional C2 assets (even just for information collection, not degradation) and tended to disapprove of these options even when critical gaps on adversary decisionmaking significantly impeded crisis management. This tended to lead to very expansive guardrails and often included that any cyber actions taken to degrade an adversary's SA must be reversible and overt to prevent misinterpretation of the purpose of the attack.

"NICE TO HAVES" VERSUS "GOTTA HAVES"

Policy teams expressed frustration with the inability of technical collectors to clearly articulate detailed value propositions associated with each collection capability. They posed questions such as, what information will I gain from capability X that I cannot get from a less risky option like Y? What will it cost? What are the trade-offs? Some of the questioning betrayed the bounds of scenario-based discussions or exercises in which the policy group had to make decisions based on the limited information available, but the interrogative nature of the exchange and repeated requests for more "homework" appeared to replicate potential real-world crises in which decisionmakers seek higher confidence information at lower levels of risk and fear slippery slopes and unintended consequences that could lurk behind information collection choices they do not fully understand.

> *Generally, policy groups viewed new and unfamiliar technical capabilities with higher levels of mistrust and with keen attention to perceived escalation risks.*

Generally, policy groups viewed new and unfamiliar technical capabilities with higher levels of mistrust and with keen attention to perceived escalation risks. Policy teams often epitomized generational and experiential gaps compared to tech collectors and hence a slightly lower "technology IQ" that manifested in higher concerns about the utility and risks of these capabilities. Due to their different knowledge base, they demonstrated a subsequent lesser comfort level with deploying emerging technologies. Policy groups also tended to assume a higher likelihood of technology failure (worst-case scenario decisionmaking), while technical groups generally held high confidence in the capability to perform as intended and approached information collection from an optimization perspective.

"BUT WHAT DOES THIS SIGNAL?"

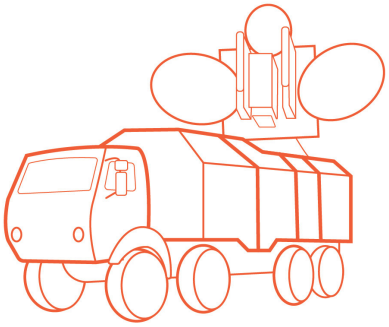
Juxtaposed with policy teams, tech group participants were largely indifferent to the signaling that accompanies the deployment of certain technologies. In stark contrast, signaling was often a primary subject of discussion for policy teams, whose comments often underscored the perceived

Juxtaposed with policy teams, tech group participants were largely indifferent to the signaling that accompanies the deployment of certain technologies.

inextricability between collection and signaling. Policy teams recognized that SA capabilities are primarily for information collection but clarified that if they were to be employed in a signaling capacity, this would have to be made clear in order to prevent inadvertent escalation. That is why caveats were often added to approved capabilities. For example, even when smallsats were overwhelmingly approved, policymakers advocated that their deployment be accompanied by a diplomatic message.

Not only were policy participants concerned with the signals that their actions conveyed to the adversary and allies, but they also repeatedly attempted to decipher the signal that an adversary was relating to them. For example, what was China signaling when it spoofed and jammed U.S. SA capabilities? For some individuals and policy groups that believed in a more assertive military posture, SA capabilities were to be deployed to signal resolve. This was perhaps most evident when participants played the North Korea scenario: some participants expressed the belief that recent developments already signaled the resumption of military hostilities, with some even going so far as to consider whether these SA capabilities should be offensive as opposed to merely intended for increasing SA (for example, weaponizing cyber espionage to introduce malicious code into North Korean networks).

Related to the topic of signaling, concerns about North Korea's nuclear capabilities were acute, but participants showed less regard for establishing guardrails around North Korea's nuclear command, control, and communication (NC3) systems. While there was discussion around the sensitivity of these systems, as well as monitoring launch sites and nuclear warhead facilities, several participants diminished the threat of miscalculation or misinterpretation. One participant argued it would be "deeply irresponsible" to avoid gathering as much information as possible about North Korean nuclear capabilities considering the risks, and several others commented that given their provocative actions, North Korean leadership likely already assumed that the United States would be targeting their NC3 systems. Since the North Korea scenario reflected a fairly advanced crisis with a much more inferior adversary, policy groups seemed willing to take higher levels of risk, with one participant explaining their logic as a concern not over the riskiness about any one capability but rather the usefulness of the information currently. That said, these discussions were among the most contentious and the approval decisions were far from unanimous.



6 | The Way Ahead

In crises between nuclear powers, the nuclear shadow will loom large. The emerging situational awareness (SA) ecosystem can create new risks but can also ameliorate them depending on how these capabilities are used and communicated. Indeed, finding a balance between risk and benefit in such a complex security environment while also maximizing the value of information to terminate a crisis or conflict on favorable terms will not happen automatically. This environment will also require new perspectives on the value and risks associated with information dominance and its impact on nuclear crises. Information dominance has been essential to ensuring U.S. military effectiveness, but in a combined conventional/nuclear ecosystem involving conflict between nuclear-armed adversaries, the picture is far more complex.

In the emerging strategic SA ecosystem, new technologies are transforming the way information is collected, analyzed, and acted upon during competition between rival states. The growing reliance on technology across the spectrum of conflict means decisionmakers will have to grapple with enormous amounts of information from widely varying and potentially unfamiliar sources and on compressed timeframes. This increasingly combined strategic SA ecosystem, including a wide array of SA technologies, along with critical enablers, can create uncertainty in the conventional and nuclear space that could create escalatory risks under crisis scenarios. Advances in numerous technologies, however, have vastly increased the importance of SA for conventional conflict, including through remote sensing, global positioning system (GPS) navigation, internet communications, cyber capabilities, and remotely piloted unmanned vehicles, among others. Today these systems are substantially more capable, but the increased speed and precision is accompanied by a lack of firebreaks that could slow crises from escalating to nuclear conflict.

The transformational nature of the strategic SA landscape suggests a second look is necessary to consider the risks these emerging capabilities may introduce as well as and the challenges they may pose for policy professionals, especially when employed in a crisis or conflict between nuclear-armed states. To effectively manage crisis escalation, decisionmakers must understand how the strategic SA ecosystem has evolved, appreciate the dynamic relationship between improved strategic SA and crisis stability, and recognize the complex interplay between technology, escalation, and decisionmaking. This report has tried to take an initial step toward that reconsideration and examine the characteristics of this new environment and its implications.

Key Conclusions

The growing nuclear shadow requires new perspectives on the value and achievability of information dominance.

As the risk of crisis between nuclear-armed adversaries increases, assumptions about the value and achievability of information dominance may need to be reconsidered. Information dominance has been essential to ensuring U.S. military effectiveness, sustaining the credibility and assurance of military alliances, and stabilizing or reducing the risks of miscalculation or collateral damage, especially in post-Cold War conventional conflicts. In the combined conventional-nuclear strategic SA ecosystem, surveillance capabilities vital to U.S. conventional superiority may introduce underappreciated escalatory risks and anxieties. Careful re-examination is required.

The risk of inadvertent escalation will dominate how decisionmakers think about a crisis between nuclear-armed states. The presence of new technologies can enhance SA and influence risk perceptions, both positively and negatively. New technologies can provide more information more quickly and with greater precision than ever before, but decisionmakers must weigh the benefits of more rapid, decisive military victory afforded by information dominance against the high-stakes risks of possible nuclear escalation. Escalation anxiety may make decisionmakers assess the value of information and the means of its collection differently and with greater caution.

Critical decisions necessary to achieve and manage information dominance will occur early in a crisis as both sides seek to understand and resolve the crisis on the most favorable terms possible. Effective tools to evaluate risk, utility, and confidence associated with strategic SA capabilities are lacking, especially early in a crisis when the situation is most uncertain and information demands are high.

Despite the potential value of enhanced SA, decisionmakers may reject certain capabilities during a crisis if they perceive them as provocative or escalatory. Escalation aversion could result in information gaps during a crisis, contributing to strategic surprise, deterrence failure, or miscalculation. This could create new, unanticipated paths toward escalation or alternatively lead decisionmakers to "micromanage" their use. This could also exacerbate tensions between policymakers and operators, whose needs and perspectives on the value of supplemental information may differ.

The combined conventional/nuclear strategic SA ecosystem is here to stay.

Comingled platforms, mutual dependencies between conventional and non-conventional capabilities, and the need for strategic SA capabilities to address nuclear risks preclude relying on "disentanglement" as a primary means of risk reduction. Many technologies (e.g., AI, advanced sensors, autonomous unmanned platforms) will be comingled and integrated on single platforms, as well as interchangeable across platforms, requiring new frameworks and lexicons to understand the potential strategic risks and benefits of using them. Nuclear and conventional missions will be distinguished less by the capabilities used and more by the missions to which they are assigned.

The strategic SA ecosystem may be combined across the conventional and nuclear realms, but the communities responsible for planning, policy, and crisis management in these two operational areas are not. That needs to change. Communication and collaboration across both communities is essential to understand the trade-offs, risks, and benefits to conventional-nuclear integration in the strategic SA arena.

Nuclear and conventional communities—military and civilian—bring different perspectives, familiarity, and comfort with different technical capabilities and in turn will raise different questions and maintain different assumptions about the risks and benefits of their use. Managing conventional crisis under a nuclear shadow will require an appreciation for these differences and a combined approach.

The combined nuclear/conventional strategic SA ecosystem will shape, not just inform, crises with nuclear-armed states.

Strategic SA capabilities, especially when used overtly, can signal U.S. intent to an adversary, predict adversary action, manage allies and partners, and shape the international environment more broadly. On the other hand, tactical or operational collection decisions—such as where unmanned aircraft can fly or which cyber systems will be penetrated—will be infused with strategic meaning and consequences.

The United States will need to weigh when, whether, and how to share information regarding the use of new strategic SA technologies with allies and partners in a crisis. This will include questions regarding the disclosure of covert or clandestine capabilities, operational coordination, and "rules of the road" in terms of friend-on-friend surveillance.

To improve their utility in a crisis, autonomous collection platforms (e.g., unmanned, cyber, and space-based systems) must be able to adapt to various policy-imposed limits. Intrusive or clandestine capabilities are most likely to be subject to policy constraints or "guardrails" to limit where, when, or how such capabilities can be used or to establish specific high-level approval processes. At a minimum, collectors and operators must be prepared for additional transparency and disclosure requirements, and policymakers need a clear understanding of the costs, as well as benefits, associated with such constraints.

High stakes and unfamiliar technologies may increase the risk of biased decisionmaking.

Cognitive bias—a looming challenge for all decisionmakers—may be exacerbated in the emerging strategic SA ecosystem, with unfamiliar technology and high-stakes, high-stress circumstances. Training and preparation can reduce the influence of cognitive biases and improve the decision process regarding the use of information collection capabilities in a crisis, but only if done in advance.

Decisionmakers have few tools to understand how nuclear-armed adversaries perceive the new strategic SA environment, technologies, and their linkages with escalation and risk. As a result, decisionmakers are forced to make assumptions—assumptions an adversary might not share. In the absence of data, decisionmakers look for definable boundaries (e.g., international borders) that may reflect Western values and biases. Filling these gaps should be a priority for future research and a topic for dialogue with both allies and potential adversaries.

The vulnerabilities of some technical capabilities to interference, manipulation, disinformation, spoofing, or even cooptation by an adversary are not well understood, especially in the areas of cyber, space, and AI. Under such high-stakes scenarios, decisionmakers will demand high confidence in informational provenance and chain of custody.

How emerging strategic SA technologies are used in peacetime, or in early crises, will have significant bearing on decisionmakers' perspectives and familiarity regarding their acceptable use in crisis and war. Introducing new or unfamiliar capabilities in crisis will prompt additional scrutiny for utility and escalatory risk. Finding ways to utilize these capabilities to enhance strategic SA before a crisis will improve familiarity and may reduce perceived escalatory risks.

Recommendations

Close the divide between technology and policy regarding the benefits, risks, and requirements for strategic SA capabilities. Information complexity and a lack of familiarity with strategic SA capabilities introduces underappreciated risks, especially in high-stakes, high-stress scenarios under a nuclear shadow. Technical, operational, and policy communities lack common views on the utility of some capabilities, the risks of disclosure, and the provocation involved in their use, as well as their vulnerability to tampering or manipulation. Socializing technical capabilities and operational requirements now—through training, exercises, and simulations as well as day-to-day use for strategic SA—is essential to reducing information risks, minimizing cognitive biases, and improving crisis management.

Integrate strategy, planning, and operations between the conventional and nuclear communities to better prepare for conventional crises under a nuclear shadow. These integrated approaches must incorporate early-crisis scenarios and recognize the combined strategic SA ecosystem that supports both nuclear and conventional missions. Differing perspectives on information dominance, escalation anxiety, and transparency need to be appreciated and adjudicated in advance.

Engage with allies and potential adversaries on issues of technology, information, and warning to better understand thresholds, risks, and perceptions in early crisis. The "information space" is underappreciated and critical for understanding and managing crises, not only in terms of internal decisionmaking but also externally with partners and potential adversaries. Multilateral planning and exercises with allies and partners should incorporate informational aspects of early crisis management. Similarly, issues of escalatory risks associated with warning, surveillance, and information should be addressed through security and stability dialogues with potential adversaries.

Seek ways to make strategic SA capabilities and the information they provide more adaptable and flexible to potential requirements for enhanced transparency, signaling, self-attribution, information sharing, and public disclosures. This may include the development of mechanisms, protocols, and options needed to manage collection assets beyond traditional covert, clandestine, or intelligence-oriented concepts of operation when needed for signaling and crisis management purposes in a crisis with a nuclear-armed adversary.

About the Authors

Rebecca Hersman is director of the Project on Nuclear Issues and senior adviser for the International Security Program at CSIS. Ms. Hersman joined CSIS in April 2015 from the Department of Defense (DOD), where she served as deputy assistant secretary of defense for countering weapons of mass destruction (WMD) since 2009. In this capacity, she led DOD policy and strategy to prevent WMD proliferation and use, reduce and eliminate WMD risks, and respond to WMD dangers. Ms. Hersman was a key leader on issues ranging from the nuclear security summit to the elimination of Syria's chemical weapons to the global health security agenda. She served as the DOD's principal policy advocate on issues pertaining to the Biological Weapons Convention, the Chemical Weapons Convention, the Nuclear Non-Proliferation Treaty, and the Cooperative Threat Reduction Program. Prior to joining the DOD, Ms. Hersman was a senior research fellow with the Center for the Study of Weapons of Mass Destruction at the National Defense University from 1998 to 2009. Her primary projects focused on the role of the DOD in mitigating the effects of chemical and biological weapons attack, concepts and strategies for eliminating an adversary's WMD programs, and proliferation issues facing the United States. Ms. Hersman also founded and directed the WMD Center's Program for Emerging Leaders, an initiative designed to shape and support the next generation of leaders from across the U.S. government with interest in countering weapons of mass destruction. Ms. Hersman previously held positions as an international affairs fellow at the Council on Foreign Relations, a special assistant to the undersecretary of defense for policy, and a member of the House Armed Services Committee professional staff. She holds an MA in Arab studies from Georgetown University and a BA from Duke University.

Reja Younis is a program manager and research associate with the Project on Nuclear Issues in the International Security Program at CSIS. Prior to working at CSIS, she completed a year-long fellowship with the Stimson Center, where she conducted research on nuclear deterrence challenges, crisis dynamics, and great power competition in the context of South Asia. She has also worked as a research analyst for the Chicago Project on Political Violence and has served as an editorial writer and subeditor of the Opinion and Editorial section for the Tribune newspaper. She holds a bachelor's degree in social sciences and liberal arts from the Institute of Business Administration Karachi and a master's degree in international relations from the University of Chicago.

Bryce Farabaugh is a research intern with the Project on Nuclear Issues in the International Security Program at CSIS. Prior to joining CSIS, Bryce held positions as a research intern at the Center for Arms Control and Non-Proliferation and a policy intern with the Defense and Foreign Policy Department at the Niskanen Center and worked for several years at the United States Department of the Treasury. He graduated cum laude from the University of Washington after three years of study with a BA in political science and department options in international security and political economy.

Bethany L. Goldblum is an associate research engineer in the Department of Nuclear Engineering at the University of California, Berkeley. Goldblum also serves as executive director for the Nuclear Science and Security Consortium, a multi-institution initiative established by the Department of Energy's National Nuclear Security Administration to conduct research and development supporting the nation's nonproliferation mission while expanding the talent pipeline. Her research explores fundamental and applied nuclear physics, scintillator characterization, multi-source analytics, experimental wargaming, and nuclear security policy. Goldblum leads the Bay Area Neutron Group, a research team focused on applied neutron physics for nuclear security applications, and founded and directs the Nuclear Policy Working Group, an interdisciplinary team of scholars developing

policy solutions to strengthen global nuclear security. She has been involved with the Public Policy and Nuclear Threats Boot Camp nearly since its inception and acted as director of the program since 2014. Goldblum maintains active collaborations with the U.S. DOE National Laboratories and is an affiliate at Lawrence Berkeley, Lawrence Livermore, and Sandia National Laboratories. She is author or co-author of more than 60 scientific publications. Goldblum received a PhD in Nuclear Engineering from the University of California, Berkeley.

Andrew Reddie is a postdoctoral research fellow at the University of California, Berkeley. Previously, Andrew received his doctorate from the Charles and Louise Travers Department of Political Science at the University of California, Berkeley. He currently serves as deputy director for the Nuclear Policy Working Group and as a researcher for the Department of Nuclear Engineering, Goldman School of Public Policy, Center for Long-Term Cybersecurity, and Berkeley Asia-Pacific Study Center at UC Berkeley as well as a researcher with the Project on Nuclear Gaming. He is also a Nuclear Science and Security Consortium (NSSC) fellow and Bridging the Gap (BtG) fellow. He holds an MPhil in International Relations from Oxford University as well as an MA and a BA (hons.) from the University of California, Berkeley. Andrew has also held research and editorial roles at the Center for Global Security Research at Lawrence Livermore National Laboratory, Business and Politics, the Canadian International Council, and the Council on Foreign Relations in Washington, D.C. Andrew's work has appeared in a variety of academic and policy-oriented publications, including Science, Journal of Cyber Policy, and the Bulletin of Atomic Scientists.

Endnotes

1 One example is the U.S. Ballistic Missile Early Warning System (BMEWS), which became operational beginning in 1959 and was designed to detect incoming Soviet ICBMs with a network of radars placed in Alaska, Greenland, and the United Kingdom—well outside of Soviet territory.

2 John A. Ardis and Shima D Keene, *Maintaining Information Dominance in Complex Environments* (Carlisle, PA: U.S. Army War College, Strategic Studies Institute, October 2018), https://publications.armywarcollege.edu/pubs/3658.pdf.

3 According to the 2018 National Defense Strategy, "inter-state strategic competition, not terrorism, is now the primary concern in U.S. national security." James Mattis, *2018 National Defense Strategy of the United States of America* (Washington, DC: U.S. Department of Defense, 2018), https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

4 Ibid.

5 China is developing a more advanced mobile missile arsenal and has tasked its air force with the development of a strategic bomber to credibly complete its nuclear triad; Pakistan is building warheads with multiple independently targetable reentry vehicles (MIRV) and has significantly improved its cruise missile capability; and India is developing longer range missiles and diversifying its delivery platforms to include sub-and ship-launched ballistic missiles. See U.S. Defense Intelligence Agency (DIA), *China Military Power: Modifying a Force to Fight and Win* (Washington, DC: November 2018), https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/China_Military_Power_FINAL_5MB_20190103.pdf; Missile Defense Project, "Missiles of Pakistan," Missile Threat, CSIS, June 14, 2018, https://missilethreat.csis.org/country/pakistan/; and Missile Defense Project, "Missiles of India," Missile Threat, CSIS, June 14, 2018, https://missilethreat.csis.org/country/india/.

6 Kathleen H. Hicks et al., *By Other Means Part 1: Competing in the Gray Zone* (Washington, DC: CSIS, July 2019), https://www.csis.org/analysis/other-means-part-i-campaigning-gray-zone.

7 Isaac R. Porche, III, et al., *Data Flood: Helping the Navy Address the Rising Tide of Sensor Information* (Santa Monica, CA: RAND Corporation, 2014), https://www.rand.org/pubs/research_reports/RR315.html.

8 Amy Woolf, "Russia's Nuclear Weapons: Doctrine, Forces, and Modernization," Congressional Research Service, updated January 2, 2020, https://fas.org/sgp/crs/nuke/R45861.pdf; DIA, *China Military Power*; Missile Defense Project, "Missiles of Pakistan"; and Missile Defense Project, "Missiles of India."

9 James M. Acton, "Technology, Doctrine, and the Risk of Nuclear War," in Nina Tannenwald, James M. Acton, and Jane Vaynman, *Meeting the Challenges of the New Nuclear Age: Emerging Risks and Declining Norms in the Age of Technological Innovation and Changing Nuclear Doctrines* (Cambridge, MA: American Academy of Arts and Sciences, 2018), https://www.amacad.org/sites/default/files/publication/downloads/New-Nuclear-Age_Emerging-Risks.pdf.

10 Mark S. Bell and Julia Macdonald, "How to Think About Nuclear Crises," T*exas National Security Review* 2, no. 2 (February 2019), https://doi.org/10.26153/tsw/1944.

11 For example, early-warning satellites employed by the United States were used exclusively for detecting the launch of nuclear missiles until the 1980s. See Norman Friedman, *Seapower and Space: From the Dawn of the Missile Age to Net-Centric Warfare* (Annapolis, MA: Naval Institute Press, 2000), p. 242–245.

12 Allan S. Krass, *The United States and Arms Control: The Challenge of Leadership* (Westport, CT: Praeger, 1997).

13 Mariel Borowitz, "Strategic Implications of the Proliferation of Space Situational Awareness Technology and Information: Lessons Learned from the Remote Sensing Sector," *Space Policy* 47 (February 2019), https://doi.org/10.1016/j.spacepol.2018.05.002.

14 "Advanced Extremely High Frequency System," Air Force Space Command, March 22, 2017, https://www.afspc.af.mil/About-Us/Fact-Sheets/Display/Article/249024/advanced-extremely-high-frequency-system/

15 James Acton, Escalation through Entanglement: How the Vulnerability of Command-and-Con-

trol Systems Raises the Risks of an Inadvertent Nuclear War," *International Security* 43, no. 1 (Summer 2018), https://www.mitpressjournals.org/doi/pdf/10.1162/isec_a_00320; and Department of Defense, Nuclear Posture Review (Washington, DC: February 2018), https://media.defense.gov/2018/Feb/02/2001872886/-1/-1/1/2018-NUCLEAR-POSTURE-REVIEW-FINAL-REPORT.PDF.

16 Keir A. Lieber and Daryl G. Press, "The New Era of Counterforce: Technological Change and the Future of Nuclear Deterrence," *International Security* 41, no. 4 (April 2017): 9–49, https://doi.org/10.1162/ISEC_a_00273.

17 Ankit Panda, "The Right Way to Manage a Nuclear North Korea," *Foreign Affairs*, November 19, 2018, https://www.foreignaffairs.com/articles/north-korea/2018-11-19/right-way-manage-nuclear-north-korea.

18 Acton, "Escalation through Entanglement."

19 Robert Jervis, *Perception and Misperception in International Politics: New Edition* (Princeton University Press, 2017), https://doi.org/10.2307/j.ctvc77bx3.

20 Molly Kovite, "I, Black Box: Explainable Artificial Intelligence And The Limits Of Human Deliberative Processes," War on the Rocks, July 5, 2019, https://warontherocks.com/2019/07/i-black-box-explainable-artificial-intelligence-and-the-limits-of-human-deliberative-processes/.

21 Laura R. Marusich et al., "Effects of information availability on command-and-control decision making: Performance, trust, and situation awareness," *Human Factors* 58, no. 2 (2016): 301–321, doi:10.1177/0018720815619515.

22 James Johnson and Eleanor Krabill, "AI, Cyberspace, And Nuclear Weapons," War on the Rocks, January 31,2020, https://warontherocks.com/2020/01/ai-cyberspace-and-nuclear-weapons/.

23 Michael O'Hanlon, *Forecasting Change in Military Technology*, 2020-2040 (Washington, DC: Brooking, September 2018), https://www.brookings.edu/wp-content/uploads/2018/09/FP_20181218_defense_advances_pt2.pdf.

24 John Thornhill, "As Moore's Law Fades, Computing Seeks a New Dimension," *Financial Times*, November 6, 2018, https://www.ft.com/content/11c1e372-e106-11e8-8e70-5e22a430c1ad.

25 Sam Shead, "Researchers: Are We on the Cusp of an 'AI Winter'?," BBC News, January 12, 2020, https://www.bbc.com/news/technology-51064369.

26 Melissa Dalton et al., *By Other Means Part II: Adapting to Compete in the Gray Zone* (Washington, DC: CSIS, August 2019), https://www.csis.org/analysis/other-means-part-ii-adapting-compete-gray-zone.

27 All three distances are measured along the ground from the point directly beneath the HAPS to the location of the target. See: "Airbus Zephyr: Unique Contribution to Decision Superiority," Airbus Defence and Space, 2017, https://www.airbus.com/content/dam/corporate-topics/publications/brochures/0612_17_zephyr_datasheet_e_horizontal_a4_lowres.pdf.

28 Pedro Valdez and Paulina Wheeler, "High Altitude Pseudosatellites," On the Radar, CSIS, July 29, 2019, https://ontheradar.csis.org/issue-briefs/high-altitude-pseudosatellites/.

29 Iftikhar Ali et al., "Satellite Remote Sensing of Grasslands: From Observation to Management," *Journal of Plant Ecology* 9, no. 6 (2016): 649-71; Guijun Yang et al., "Unmanned Aerial Vehicle Remote Sensing for Field-Based Crop Phenotyping: Current Status and Perspectives," *Frontiers in Plant Science* 8 (2017): 1-26.; W. Carter Johnson et al., "Modeling Seed Dispersal and Forest Island Dynamics," in *Ecological Studies Forest Island Dynamics in Man-Dominated Landscapes*, R.L. Burgess and D.M. Sharpe, eds. (December 1981), 215-39; Jeremy H. Groves et al., "Modelling of Floating Seed Dispersal in a Fluvial Environment," *River Research and Applications*, 2009, no. 25 (2009): 582-92.

30 Jake Hecla, "Light Detection and Ranging (LIDAR)," On the Radar, CSIS, July 29, 2019, https://ontheradar.csis.org/issue-briefs/light-detection-and-ranging-lidar/.

31 "Echo Voyager," Boeing, https://www.boeing.com/defense/autonomous-systems/echo-voyager/index.page.

32 H. I. Sutton, "China Navy Reveals New Large Underwater Robot Which Could Be A Game

Changer," *Forbes*, October 1, 2019, https://www.forbes.com/sites/hisutton/2019/10/01/china-reveals-new-robot-underwater-vehicle-hsu-001/#31cd33c21991.

33 Ben Werner, "Navy's Knifefish Unmanned Mine Hunter Passes Sea Acceptance Testing," USNI News, June 5, 2018, https://news.usni.org/2018/06/05/navys-knifefish-unmanned-mine-hunter-passes-key-test.

34 Megan Eckstein, "Boeing, Lockheed Martin Moving Forward with Navy XLUUV Acquisition Program," USNI News, October 2017, https://news.usni.org/2017/10/17/28810.

35 Nate Frierson and Lizamaria Arias, "Artificial Intelligence Analysis Applications," On the Radar, CSIS, July 29, 2019, https://ontheradar.csis.org/issue-briefs/artificial-intelligence-analysis-applications-a-technology-primer/.

36 Natalie Sherman, "Is China Gaining an Edge in Artificial Intelligence?," BBC News, November 12, 2019, https://www.bbc.com/news/business-50255191.

37 Phil Stewart, "Deep in the Pentagon, a Secret AI Program to Find Hidden Nuclear Missions," Reuters, June 5, 2018, https://www.reuters.com/article/us-usa-pentagon-missiles-ai-insight/deep-in-the-pentagon-a-secret-ai-program-to-find-hidden-nuclear-missiles-idUSKCN1J114J.

38 Cheryl Pellerin, "Project Maven to Deploy Computer Algorithms to War Zone by Years End," DoD News, Defense Media Activity, July 21, 2017, https://dod.defense.gov/News/Article/Article/1254719/project-maven-to-deploy-computer-algorithms-to-war-zone-by-years-end/.

39 Stewart, "Deep in the Pentagon."

40 Lora Saalman, ed., *The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk: East Asian Perspectives*, Vol. 2, (Stockholm, Sweden: Stockholm International Peace Research Institute, October 2019), https://www.sipri.org/publications/2019/other-publications/impact-artificial-intelligence-strategic-stability-and-nuclear-risk-volume-ii.

41 Amy Butler and Bill Sweetman, "Secret New UAS Shows Stealth, Efficiency Advances," *Aviation Week & Space Technology*, December 6, 2013, http://aviationweek.com/defense/secret-new-uas-shows-stealth-efficiency-advances.

42 Richard Tompkins. "BAE Systems developing new sonar for U.S. Navy submarines," UPI, July 18, 2017, https://www.upi.com/Defense-News/2017/07/18/BAE-Systems-developing-new-sonar-for-US-Navy-submarines/3081500391180/.

43 Frederic Bouchard et al., "High-dimensional quantum cloning and applications to quantum hacking," *Science Advances* 3, no. 2, (February 2017), doi:10.1126/sciadv.1601915.

44 It is important to note that different names do not necessarily denote separate entities. See "Lazarus Group," MITRE, ATT&CK, accessed February 19, 2020, https://attack.mitre.org/groups/G0032/; Nalani Fraser "APT38: Details on New North Korean Regime-Backed Threat Group," FireEye, October 3, 2018, https://www.fireeye.com/blog/threat-research/2018/10/apt38-details-on-new-north-korean-regime-backed-threat-group.html; "North Korean Malicious Cyber Activity," CISA, accessed February 19, 2020, https://www.us-cert.gov/HIDDEN-COBRA-North-Korean-Malicious-Cyber-Activity; https://securityaffairs.co/wordpress/67895/apt/north-korea-group-123.html; and Adam Meyers "Advanced Persistent Threat List: Types of Threat Actors," CrowdStrike, December 12, 2019, https://www.crowdstrike.com/blog/meet-the-adversaries/.

45 "North Korea's Ruling Elite Adapt Internet Behavior to Foreign Scrutiny," Recorded Future, April 25, 2018, https://www.recordedfuture.com/north-korea-Internet-behavior/.

46 Hecla, "Light Detection and Ranging (LIDAR).".

47 Lieber and Press, "The New Era of Counterforce.".

48 Wang Yi, "ADASpace set to star in AI satellite constellation sphere," *Global Times*, June 30, 2019, http://www.globaltimes.cn/content/1156263.shtml.

49 Valdez and Wheeler, "High Altitude Pseudosatellites."; See example: United Kingdom orders additional Zephyr," Airbus Defense and Space, August 18, 2016, https://www.airbus.com/newsroom/press-releases/en/2016/08/united-kingdom-orders-additional-zephyr.html.

50 "Beihang Successfully Researches and Develops Our Nation's First Chang Ying Large Long-En-

durance UAV" [北航成功研制我国首款长鹰大型长航时无人机], Sina, September 13, 2011, http://mil.news.sina.com.cn/2011-09-13/1345665189.html; Chris Biggers, "Satellite Imagery Reveals China's New Drone Base," bellingcat, June 29, 2015, https://www.bellingcat.com/news/rest-of-world/2015/06/29/satellite-imagery-reveals-chinas-new-drone-base/?utm_source=Sail-thru&utm_medium=email&utm_term=%2ASituation Report&utm_campaign=SitRep0630; Ankit Panda, "Meet China's East China Sea Drones," Diplomat, June 30, 2015, https://thediplomat.com/2015/06/meet-chinas-east-china-sea-drones/.

51 "RQ-4 Global Hawk Fact Sheet," United States Air Force, October 2014, https://www.af.mil/About-Us/Fact-Sheets/Display/Article/104516/rq-4-global-hawk/.

52 Reddie and Goldblum, "Unmanned Underwater Vehicle (UUV) Systems for Submarine Detection."

53 Stephen Chen, "China military develops robotic submarines to launch a new era of sea power," *South China Morning Post*, July 22, 2018, https://www.scmp.com/news/china/society/article/2156361/china-developing-unmanned-ai-submarines-launch-new-era-sea-power.

54 McCormick, "United States Situational Awareness."

55 Department of Defense, "Department of Defense Announces Successful Micro-Drone Demonstration," Press Release, January 9, 2017, https://dod.defense.gov/News/News-Releases/News-Release-View/Article/1044811/department-of-defense-announces-successful-micro-drone-demonstration/.

56 Ibid.

57 Andrew Reddie and Bethany Goldblum, "Smallsats," On the Radar, CSIS, May 4, 2019, https://res.cloudinary.com/csisideaslab/image/upload/v1562865065/on-the-radar/Smallsats%20Final%20Primer%20Formatted%2007-02-29.pdf.

58 McCormick, "United States Situational Awareness."

59 U.S. Army Training and Doctrine Command, *The U.S. Army in Multi-Domain Operations 2028* (Fort Eustis, VA: December 2018), https://info.publicintelligence.net/USArmy-MultidomainOps2028.pdf.

60 Elsa Kania, "China's Strategic Situational Awareness Capabilities," On the Radar, Center for Strategic and International Studies, July 29, 2019, https://ontheradar.csis.org/issue-briefs/china-situational-awareness/.

61 Ibid.

62 Ibid.

63 From a forthcoming primer to be published on the On the Radar website by Jason Arterburn.

64 James M. Acton, "Reclaiming Strategic Stability," in *Strategic Stability: Contending Interpretations*, Elbridge A. Colby and Michael S. Gerson, eds., (Carlisle Barracks, PA: Strategic Studies Institute, 2014), 117–146.

65 Thomas C. Schelling, *The Strategy of Conflict* (Cambridge, MA: Harvard University Press, 1980).

66 Acton, "Reclaiming Strategic Stability."

67 Paul Scharre and Michael C. Horowitz, *Artificial Intelligence: What Every Policymaker Needs to Know* (Washington, DC: Center for a New American Security, 2018), https://www.cnas.org/publications/reports/artificial-intelligence-what-every-policymaker-needs-to-know. .

68 Ibid.

69 Robert Jervis, "Cooperation Under the Security Dilemma," World Politics 30, no. 2 (1978): 167-214, accessed February 10, 2020, www.jstor.org/stable/2009958.

70 Todd Harrison, Kaitlyn Johnson, and Thomas G. Roberts, *Space Threat Assessment 2019* (Washington, DC: CSIS, April 2019), https://www.csis.org/analysis/space-threat-assessment-2019.

71 Austin Long and Brendan Rittenhouse Green, "Stalking the Secure Second Strike: Intelligence, Counterforce, and Nuclear Strategy," *Journal of Strategic Studies* 38, no. 1-2 (2015): 38-73, https://www.tandfonline.com/doi/pdf/10.1080/01402390.2014.958150.

72 Michael E. Devine, "Covert Action and Clandestine Activities of the Intelligence Community:

Selected Definitions in Brief," Congressional Research Service, June 14,2019, https://fas.org/sgp/crs/intel/R45175.pdf

73 Ibid.

74 Benjamin, "Plant-based Sensors."

75 Brian Martin, "Technological Vulnerability," *Technology in Society* 12, no. 4 (1996): 511-523, https://documents.uow.edu.au/~bmartin/pubs/96tis.html.

76 "Summary: Department of Defense Cyber Strategy 2018," DOD, September 2018, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

77 Robert Jervis and Mira Rapp-Hooper, "Perception and Misperception on the Korean Peninsula: How Unwanted Wars Begin," *Foreign Affairs*, June 2018, https://www.foreignaffairs.com/articles/north-korea/2018-04-05/perception-and-misperception-korean-peninsula.

78 John J. Mearsheimer, "Chapter 2: Anarchy and the Struggle for Power," in *The Tragedy of Great Power Politics*, 1st ed., The Norton Series in World Politics (New York, NY: Norton, 2001).

79 John H. Herz, *Political Realism and Political Idealism: A Study in Theories and Realities* (Chicago: University of Chicago Press, 1951).

80 Robert Jervis, "War and Misperception," *Journal of Interdisciplinary History* 18, no. 4 (1988): 675, https://doi.org/10.2307/204820.

81 Brian A. Jackson et al., *Evaluating Novel Threats to the Homeland: Unmanned Aerial Vehicles and Cruise Missiles* (Santa Monica, Calif.: RAND Corporation, 2008), https://www.rand.org/pubs/monographs/MG626.html.

82 Richard Leiby, "U.N.: U.S. Drone Strikes Violate Pakistan Sovereignty," *Washington Post*, March 15, 2013, https://www.washingtonpost.com/world/asia_pacific/un-us-drones-violate-pakistan-sovereignty/2013/03/15/308adae6-8d8a-11e2-adca-74ab31da3399_story.html.

83 Jim Garamone, "Iran Shoots Down U.S. Global Hawk Operating in International Airspace," U.S. Department of Defense, June 20, 2019, https://www.defense.gov/Explore/News/Article/Article/1882497/iran-shoots-down-us-global-hawk-operating-in-international-airspace/.

84 Donald J. Trump, Twitter post, June 21, 2019, 6:03 AM, https://twitter.com/realDonaldTrump/status/1142055375186907136.

85 Karsten Geier et al., *Moving Beyond Cyber Wars: A Translatlantic Dialogue* (Washington, DC: American Institute for Contemporary German Studies, Johns Hopkins University, September 2018), AICGS Policy Report, https://www.aicgs.org/2018/09/where-does-cyber-defense-stop-and-offense-begin/.

86 Robert Jervis, "On the Current Confrontation with Iran," War on the Rocks, January 9, 2020, https://warontherocks.com/2020/01/on-the-current-confrontation-with-iran/.

87 Geier et al., *Moving Beyond Cyber Wars.*

88 Robert Fanelli, "Cyberspace Offense and Defense," *Journal of Information Warfare* 15, no. 2 (2016): 53–65, https://www.jstor.org/stable/26487531?seq=1.

89 Tom Uren, Fergus Hanson, and Bart Hogeveen, "Defining Offensive Cyber Capabilities," International Cyber Policy Centre, Australian Strategic Policy Institute, July 4, 2018, https://www.aspi.org.au/report/defining-offensive-cyber-capabilities; and Gregory Rattray and Jason Healey, "Categorizing and Understanding Offensive Cyber Capabilities and Their Use," in *Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy* (Washington, DC: National Academies Press, 2010), https://www.nap.edu/catalog/12997/proceedings-of-a-workshop-on-deterring-cyberattacks-informing-strategies-and.

90 Lieber and Press, "The New Era of Counterforce."

91 Glenn Kent, Randall DeValk, and David Thaler, *A Calculus of First-Strike Stability* (Santa Monica, CA: RAND Corporation, 1988), https://www.rand.org/pubs/notes/N2526.html; Bell and Macdonald, "How to Think About Nuclear Crises."

92 Thomas C. Schelling, *The Strategy of Conflict* (Cambridge, MA: Harvard University Press, 1981), https://www.hup.harvard.edu/catalog.php?isbn=9780674840317.

93 Gregory H. Canavan, *Stability of Nuclear and General-Purpose Forces* (Los Alamos, NM: Los Alamos National Laboratory, 1997), http://library.sciencemadness.org/lanl2_a/lib-www/la-pubs/00412839.pdf.

94 Goldblum and Reddie, "Smallsats."

95 Sean Cate and Jesse Sloman, "Operating Under Constant Surveillance," *U.S. Naval Institute Proceedings* 142, iss. 5, no. 1,359 (May 2016), https://www.usni.org/magazines/proceedings/2016/may/operating-under-constant-surveillance.

96 Lieber and Press, "The New Era of Counterforce."

97 Austin Long and Brendan Rittenhouse Green, "Stalking the Secure Second Strike: Intelligence, Counterforce, and Nuclear Strategy," *Journal of Strategic Studies* 38, no. 1–2 (January 2, 2015): 38–73, https://doi.org/10.1080/01402390.2014.958150.

98 Lieber and Press, "The New Era of Counterforce."

99 Peter D. Feaver, "Command and Control in Emerging Nuclear Nations," *International Security* 17, no. 3 (1992/93): 165, doi:10.2307/2539133.

100 Vipin Narang, "War of the Words: North Korea, Trump, and Strategic Stability," Nuclear Security Working Group, n.d., https://nuclearsecurityworkinggroup.org/asia/war-of-the-words-north-korea-trump-and-strategic-stability/.

101 Lieber and Press, "The New Era of Counterforce."

102 James Acton, ed., *Entanglement: Russian and Chinese Perspectives on Non-Nuclear Weapons and Nuclear Risks* (Washington, DC: Carnegie Endowment for International Peace, November 2017), https://carnegieendowment.org/2017/11/08/entanglement-chinese-and-russian-perspectives-on-non-nuclear-weapons-and-nuclear-risks-pub-73162.

103 Friedman, *Seapower and Space*, 242–245.

104 Krass, T*he United States and Arms Control*.

105 Missile Defense Project, "Space-based Infrared System (SBIRS)," Missile Threat, CSIS, August 11, 2016, last modified June 15, 2018, https://missilethreat.csis.org/defsys/sbirs/.

106 James Acton ed., *Entanglement: Russian and Chinese Perspectives on Non-Nuclear Weapons and Nuclear Risks*.

107 "Global Hawk Enterprise," Northrop Grumman, n.d., https://www.northropgrumman.com/air/global-hawk-enterprise/.

108 Lieber and Press, "The New Era of Counterforce."

109 Evan Lisman, "Non-Acoustic Submarine Detection," *On the Radar*, CSIS, November 5, 2019, https://res.cloudinary.com/csisideaslab/image/upload/v1574455202/on-the-radar/Non-acoustic_Sub_Detection_Primer_c7ntof.pdf.

110 Missile Defense Project, "Ground-based Midcourse Defense (GMD) System."

111 Stephen M. McCall, "Defense Primer: Ballistic Missile Defense," Congressional Research Service, October 9, 2019, https://crsreports.congress.gov/product/pdf/IF/IF10541.

112 Missile Defense Project, "Terminal High Altitude Area Defense (THAAD)," Missile Threat, CSIS, June 14, 2018, last modified June 15, 2018, https://missilethreat.csis.org/system/thaad/.

113 Ethan Meick and Nargiza Salidjanova, "China's Response to US-South Korean Missile Defense System Deployment and Its Implications," United States-China Economic and Security Review Commission, June 26, 2017, https://www.uscc.gov/sites/default/files/Research/Report_China's%20Response%20to%20THAAD%20Deployment%20and%20its%20Implications.pdf.

114 Curtis Peebles, *High Frontier: The U.S. Air Force and the Military Space Program* (Washington, DC: Air Force Historical Studies Office, January 1997), p. 44–52.

115 Acton, "Escalation through Entanglement."

116 Fang Yong, "2015 年世界武器装备与军事技术发展重大动向" [Major trend of military equipment and technology development in the world in 2015], 军事文摘 [Military Digest], no. 23 (2015); and Deng Sijia, "美研发反导新技术：无人机发射激光 敌发射前打击" [U.S. develops new anti-mis-

sile technologies: UAV-borne laser and left of launch], PLA Daily, October 28, 2016.

117 Hamilton and Kreuzer, "The Big Data Imperative: Air Force Intelligence for the Information Age," *Air and Space Power Journal* 32, no. 1 (Spring 2018), https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-32_Issue-1/F-Hamilton_Kreuzer.pdf.

118 Porche et al., *Data Flood*.

119 Errol R. Iselin, "The Effects of the Information and Data Properties of Financial Ratios and Statements on Managerial Decision Quality," *Journal of Business Finance and Accounting* 20, no. 2 (January 1993), doi:10.1111/j.1468-5957.1993.tb00663.x.

120 Ibid.

121 Richard K. Betts, "Analysis, War, and Decision: Why Intelligence Failures Are Inevitable." *World Politics* 31, no. 1 (1978): 61-89. Accessed March 2, 2020. doi:10.2307/2009967.

122 Benjamin Schneider, "The People Make the Place," *Personnel Psychology* 40, no. 3 (September 1987): 437-453, doi:10.1111/j.1744-6570.1987.tb00609.x.

123 David Bawden, "Information and digital literacies: a review of concepts," *Journal of Documentation* 57, no. 2 (April 2001): 218-259, doi:10.1108/EUM0000000007083.

124 Hamilton and Kreuzer, "The Big Data Imperative."

125 Martin J. Eppler and Jeanne Mengis, "The Concept of Information Overload: A Review of Literature from Organization Science, Accounting, Marketing, MIS, and Related Disciplines," *Information Society* 20, no. 5 (November 2004): 325–44, https://doi.org/10.1080/01972240490507974.

126 David Bawden and Lyn Robinson, "The Dark Side of Information: Overload, Anxiety and Other Paradoxes and Pathologies," *Journal of Information Science* 35, no. 2 (April 2009): 180–91, https://doi.org/10.1177/0165551508095781.

127 Jacob Jacoby, "Information Load and Decision Quality: Some Contested Issues," J*ournal of Marketing Research* 14, no. 4 (November 1977): 569, https://doi.org/10.2307/3151201; Jacob Jacoby, "Perspectives on Information Overload," Journal of Consumer Research 10, no. 4 (March 1984): 432, https://doi.org/10.1086/208981.

128 Eppler and Mengis, "The Concept of Information Overload"; Bawden and Robinson, "The Dark Side of Information"; Nathan McNeese, Verica Buchanan, and Nancy Cooke, "The cognitive science of intelligence analysis," *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* 59 (2005): 826–830, doi:10.1177/1541931215591250.

129 Marusich et al., "Effects of information availability on command-and-control decision making."

130 Cindy Dietrich, "Decision Making: Factors that Influence Decision Making, Heuristics Used, and Decision Outcomes," *Inquiries Journal/Student Pulse* 2, no. 2 (2010), http://www.inquiriesjournal.com/a?id=180.

131 Dima Adamsky, *The Culture of Military Innovation: the Impact of Cultural Factors on the Revolution in Military Affairs in Russia, the US, and Israel* (Stanford, CA: Stanford University Press, 2010).

132 Eric Schmidt, "Statement of Dr. Eric Schmidt House Armed Services Committee April 17, 2018," Statement before the House Armed Services Committee, April 17, 2018, https://docs.house.gov/meetings/AS/AS00/20180417/108132/HHRG-115-AS00-Wstate-SchmidtE-20180417.pdf.

133 KMPG International Data and Analytics, *Guardians of trust: Who is responsible for trusted analytics in the digital age?* (Amstelveen, Netherlands: KMPG, February 2018), https://assets.kpmg/content/dam/kpmg/xx/pdf/2018/02/guardians-of-trust.pdf.

134 Daniel S. Hoadley and Kelley M. Sayler, "Artificial Intelligence and National Security," Congressional Research Service, updated November 21, 2019, https://fas.org/sgp/crs/natsec/R45178.pdf.

135 Robert D. Putnam, "Diplomacy and Domestic Politics: The Logic of Two-Level Games," *International Organization* 42, no. 3 (1988): 427-60, www.jstor.org/stable/2706785.

136 Michael C. Horowitz and Lauren Kahn, "The AI Literacy Gap Hobbling American Officialdom," War on the Rocks, January 14, 2020, https://warontherocks.com/2020/01/the-ai-literacy-gap-hobbling-american-officialdom/.

137 James Johnson and Eleanor Krabill, "AI, Cyberspace, and Nuclear Weapons," War on the Rocks, January 31, 2020, https://warontherocks.com/2020/01/ai-cyberspace-and-nuclear-weapons/.

138 Christopher W. Lum and Blake Waggoner, "A Risk Based Paradigm and Model for Unmanned Aerial Systems in the National Airspace," American Institute of Aeronautics and Astronautics, 2011, http://faculty.washington.edu/lum/website_professional/publications/Lum_UAS_risk_2011.pdf.

139 Brent B. Clark, Christopher Robert, and Stephen A. Hampton, "The Technology Effect: How Perceptions of Technology Drive Excessive Optimism," *Journal of Business Psychology* 31 (2016): 87-102, https://doi.org/10.1007/s10869-015-9399-4.

140 Robert Jervis, *Perception and Misperception in International Politics: New Edition* (Princeton, NJ: Princeton University Press, 1976), doi:10.2307/j.ctvc77bx3.

141 Betts, "Analysis, War, and Decision: Why Intelligence Failures Are Inevitable."

142 Amos Tversky and Daniel Kahneman, "Judgment under Uncertainty: Heuristics and Biases," Science 185, no. 4157 (September 1974): 1124-1131, https://www.jstor.org/stable/1738360.

143 Department of Home Affairs, *Decision Making During a Crisis: A Practical Guide* (Canberra, Australia: Government of Australia, 2018), https://www.organisationalresilience.gov.au/resources/Documents/decision-making-during-a-crisis-a-practical-guide.pdf.

144 Daniel Kahneman, *Thinking, Fast and Slow* (New York: Farrar, Straus and Giroux, 2011).

145 Molly Kovite, "I, Black Box: Explainable Artificial Intelligence and the Limits of Human Deliberative Processes," War On The Rocks, 2019, https://warontherocks.com/2019/07/i-black-box-explainable-artificial-intelligence-and-the-limits-of-human-deliberative-processes/.

146 Daniel Kahneman and Amos Tversky, "Availability: A heuristic for judging frequency and probability," *Cognitive Psychology* 5, no. 2 (September 1973): 207-232, https://doi.org/10.1016/0010-0285(73)90033-9.

147 Ibid.

148 Paul Bracken, "Instabilities in the control of nuclear forces," in *Breakthrough: Emerging New Thinking—Soviet and Western Scholars Issue a Challenge to Build a World Beyond War*, Anatoly Gromyko and Martin Hellamn, eds., (New York, NY: Walker & Company, 1988).

149 C. K. Morewedge et al., "Debiasing Decisions. Improved Decision Making With A Single Training Intervention," *Policy Insights from the Behavioral and Brain Sciences* 2, no. 1 (2015): 129-140, https://openaccess.city.ac.uk/id/eprint/12324/1/Debiasing_Decisions_PIBBS.pdf.

150 Ibid.

151 T. D. Wilson and N. Brekke, "Mental contamination and mental correction: unwanted influences on judgments and evaluations," *Psychological Bulletin* 116, no. 1 (1994): 117–142, doi:10.1037/0033-2909.116.1.117.

152 Pat Croskerry, Geeta Singhal, and Silvia Marnede, "Cognitive debiasing 1: origins of bias and theory of debiasing," *BMJ Journals* 22, iss. supp. 2 (September 2013): ii58-ii64, https://qualitysafety.bmj.com/content/22/Suppl_2/ii58.full.

153 Ed McGrady, "Getting the Story Right About Wargaming," War on the Rocks, November 8, 2019, https://warontherocks.com/2019/11/getting-the-story-right-about-wargaming/.

154 Tara Law, "Iran Shot Down a $176 Million U.S. Drone. Here's What to Know About the RQ-4 Global Hawk," *Time*, June 21, 2019, https://time.com/5611222/rq-4-global-hawk-iran-shot-down/.

155 On pseudosatellites, see Pedro Vicente Valde and Paulina Wheeler, "High Altitude Pseudosatellites," On the Radar, CSIS, July 29, 2019, https://ontheradar.csis.org/issue-briefs/high-altitude-pseudosatellites/; and on smallsats, see Goldblum and Reddie, "Smallsats."

COVER PHOTO TYRONE FERNANDEZ FROM PEXELS

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

1616 Rhode Island Avenue NW
Washington, DC 20036
202 887 0200 | www.csis.org

ROWMAN & LITTLEFIELD

Lanham • Boulder • New York • London

4501 Forbes Boulevard
Lanham, MD 20706
301 459 3366 | www.rowman.