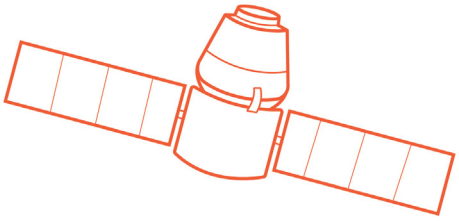


1 | Introduction

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]

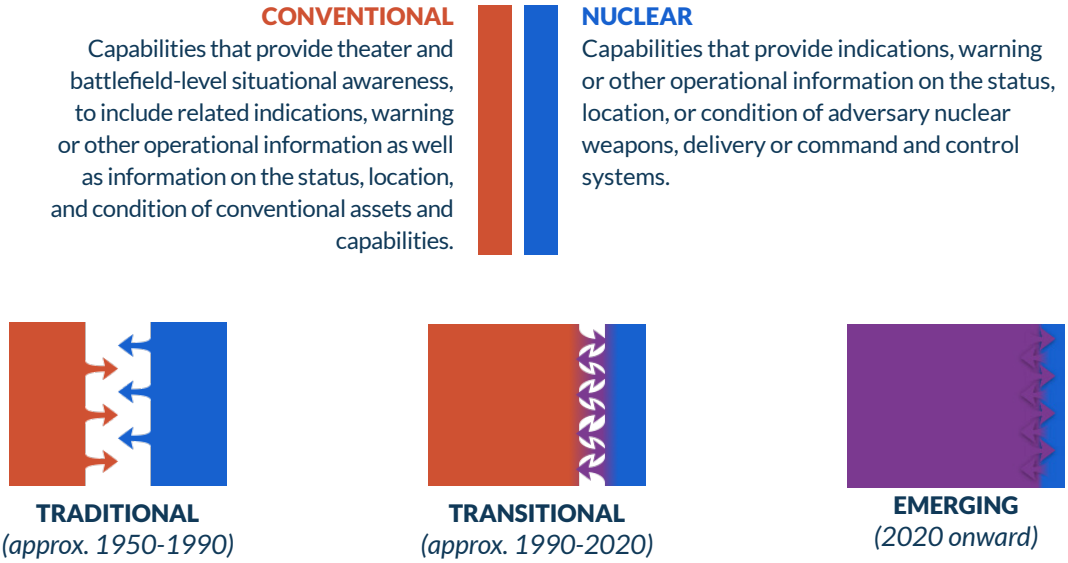
Indeed, the origin of the transitional strategic SA environment can be traced back to the 1990s. Technological developments throughout the second half of the twentieth century culminated in the networked battlefield of the Gulf War. The Gulf War saw the employment of effective communications, command, 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/)

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.