International Security at the Nuclear Nexus | Project on Nuclear Issues

JANUARY 15, 2021

# Surveillance, Situational Awareness, and Warning at the Conventional-Strategic Interface

*By* **Rebecca K.C. Hersman and Reja Younis**

For much of the nuclear age, the concepts and tools of strategic warfare—including command, control, and communications and detection, warning, and situational awareness capabilities—were distinct and highly compartmentalized from those designed to support conventional warfighting. Moreover, the systems that provided strategic nuclear warning operated at long range, from outside 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] Countries had limited incentives to target strategic warning and situational awareness systems in a conventional conflict, as doing so would not limit an adversary's ability to conduct conventional operations and would unambiguously signal the advent of a nuclear attack.

These physical and structural separations created a perceived firebreak—a barrier along the escalation ladder designed to slow or prevent accidental or automatic escalation to nuclear conflict in a conventional crisis. This notion of "firebreaking" has been integral to the theoretical underpinning of deterrence and escalation theory—including the concepts of strategic stability, secure second strike, and even the "stability-instability" paradox used to explain the coexistence of nuclear restraint and conventional aggression. Today, however, the expansion of dual-capable delivery systems and the diversification of strategic forms of warfare to include cyber, space, and advanced high precision conventional strike capabilities have sharply eroded these structural firebreaks. Just as significant, but perhaps less appreciated, are the dramatic changes in intelligence, surveillance, and reconnaissance (ISR) and the full range of systems that support strategic warning, tracking, and targeting that are increasingly combined into a single, highly capable situational awareness ecosystem that is both precise and persistent. Fueled by advances in robotics, artificial intelligence/machine learning, advanced sensor technologies, and massive growth in computing power, these highly networked, dual-capable technologies contribute to a situational awareness picture that is far more capable. But, it is also murkier and more complex in terms of understanding and managing escalation risks along the conventional/nuclear threshold. Better understanding the ways in which this new situational awareness ecosystem intersects with the nuclear mission and the benefits and risks of these emerging capabilities will be important for managing escalation under a nuclear shadow.

## Is strategic situational awareness changing?

Over time, distinctions between the upper echelons of conflict have become blurry, and pathways to escalation may be far less easily understood or defined. There are several factors driving this change. First, the capabilities designed to provide situational awareness and support senior decision-makers in crises and conflicts are more and more consolidated into a single conventional-nuclear architecture, and these cannot be disaggregated.

Dual-use strategic situational awareness (SA) capabilities may be tasked to conduct both conventional and nuclear missions in an integrated fashion. This blurring effect between the conventional and nuclear potentially creates nuclear missions for what were previously considered conventional-only capabilities. As Keir Lieber and Daryl Press suggest, increasingly capable unmanned aerial vehicles, like the Global Hawk and its advanced successors, coupled with advanced stealth and sensor capabilities may also be useful to track a small country's mobile missiles—whether nuclear or conventional—and create counterforce opportunities along the conventional/nuclear seam.[2] Tom Mahnken's work on "Deterrence by Detection" puts yet another spin on this challenge—suggesting that the

Banner Image: *An unmanned aerial vehicle delivers a payload to the ballistic missile submarine USS Henry M. Jackson around the Hawaiian Islands, Oct. 19, 2020, during an event designed to test and evaluate the tactics, techniques and procedures of U.S. Strategic Command's expeditionary logistics and enhance the readiness of strategic forces.* Source: U.S. Department of Defense

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

[2] 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 (Spring 2017): 37–46, https://doi.org/10.1162/ISEC_a_00273.

*Sailors prepare an unmanned underwater vehicle in the Persian Gulf, Dec. 6, 2018, during Mine Countermeasures Exercise 19-1, a training event with the British Royal Navy.* Source: U.S. Department of Defense, Navy Petty Officer 2nd Class Kevin J. Steinberg

extensive peacetime use of unmanned aircraft systems (UAS) surveillance may help "deter" conventional acts of aggression by China or Russia.[3] However, if such persistent capabilities deliberately or inadvertently detect and observe strategic assets, an adversary may believe that their nuclear assets are at risk, potentially escalating a crisis.

Even as modernized NC3 systems seek to ensure a "thin line" of capability is reserved exclusively to support nuclear missions under the most extreme circumstances, the vast majority of nuclear and conventional missions will rely on shared or dual-use capabilities for situational awareness, warning, and communications. This reliance on strategic warning and communication assets in conventional conflicts is on the rise. For example, conventional missile warning currently relies on dual-use surveillance capabilities, increasing the risk that the dual-use capabilities could be targeted in a conventional conflict for conventional purposes but with potentially profound strategic implications.[4] As advanced, long-range, and often dual-capable missile systems have proliferated dramatically in recent decades, including among a range of nuclear-armed adversaries, such reliance on comprehensive and integrated warning systems now must figure significantly into the planning and execution of conventional conflicts, especially when long-range strike capabilities are considered.

In addition, these systems are no longer as physically "firewalled" as in the past 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 system for strictly conventional purposes could be misconstrued as an effort to "blind" the target before launching a nuclear strike.[5] Evolving technology has also made space-based systems more vulnerable to a range of disruptive capabilities vis-à-vis spoofing, blinding, disabling, as well as with kinetic ground-based anti-satellite weapons.[6] In addition, the conventional missions of space-based capabilities suggest they could be seen as fair game for targeting in a conventional crisis or conflict. For example, the U.S. Space-Based Infrared System (SBIRS) is a

[3] Thomas G. Mahnken, Travis Sharp, Grace B. Kim, *Deterrence by Detection: A Key Role for Unmanned Aircraft Systems in Great Power Competition* (Washington, D.C.: CSBA, 2020), https://csbaonline.org/research/publications/deterrence-by-detection-a-key-role-for-unmanned-aircraft-systems-in-great-power-competition

[4] Rebecca Hersman, Reja Younis, Bryce Farabaugh, Bethany Goldblum, and Andrew Reddie, *Under the Nuclear Shadow: Situational Awareness Technology and Crisis Decisionmaking* (Washington, D.C.: CSIS, 2020), 11, https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/200318_UnderNucearShadow_FullReport_WEB.pdf?VJm_nrx2bVVeByYH38yx8YkDvvr1QZVW.

[5] James Acton, Escalation through Entanglement: How the Vulnerability of Command-and-Control Systems Raises the Risks of an Inadvertent Nuclear War," *International Security* 43, no. 1 (Summer 2018), https://www.mitpressjournals.org/doi/pdf/10.1162/isec_a_00320

[6] Todd Harrison, Kaitlyn Johnson, Thomas G. Roberts, Tyler Way, and Makena Young, Space Threat Assessment 2020 (Washington, D.C.: CSIS, 2020), https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/200330_SpaceThreatAssessment20_WEB_FINAL1.pdf?6sNra8FsZ1LbdVj3xY867tUVu0RNHw9V.

constellation of integrated satellites that enables such varied missions as providing early missile warning, cueing missile defenses, delivering technical intelligence, and supporting situational awareness.[7]

Moreover, emerging digital technologies coupled with advanced sensor and surveillance capabilities integrated across space and cyber domains can provide vast amounts of data more quickly and precisely than ever before, including information about strategic threats that may prove elusive to traditional warning systems. The United States may have to rely on conventional situational awareness systems, including systems that are more visible or intrusive to detect and warn of threats involving hypersonic weapons, boost-glide systems, long-range cruise missiles, and other capabilities that are specifically designed to elude traditional U.S. early-warning systems (e.g., radars and satellites), reduce confidence in strategic warning, and defeat U.S. missile defenses. Advanced sensor technologies and the platforms for their deployment coupled with high-bandwidth networks, quantum computing, data fusion, and artificial intelligence (AI) tools are accelerating the speed, precision, lethality, and survivability of conventional tools of warfare, potentially providing knowledge of adversary forces, deployments, and actions sooner than was previously possible.[8] Inside this dynamic situational awareness ecosystem, the already thin line between conventional and strategic stability effects—especially in terms of preserving secure second-strike confidence—is likely to erode further.

New technologies are likely to exacerbate this trend. The integration of certain artificial intelligence capabilities into the ISR fleet is already well underway. Advanced drone technology and swarming along microsatellite constellations will fundamentally change the world of surveillance. On the one hand, AI-enabled reconnaissance systems could be employed to analyze significant amounts of data and AI-augmented autonomous weapon systems will soon be deployed for surveillance and strike missions—even if used solely for conventional operations, this could create destabilizing outcomes.[9] And on the other hand, when AI enhances autonomy and sensor fusion, it may subsequently enable breakthroughs in tracking and targeting in antisubmarine warfare, or make it easier for high-precision conventional munitions to destroy hardened ICBM silos. These advancements might erode the means by which nuclear powers guarantee survivability of their nuclear forces.[10]

## What does this say about escalation and stability when crises occur under a nuclear shadow?

Whether such advanced surveillance, detection, and warning capabilities enable strategic missions or enhance strategic effects of conventional missions, these dual-use capabilities contribute to the blurring of the line between conventional and nuclear spheres. They also challenge traditional notions of stability in cases where vertical and horizontal escalation converge, potentially opening unexpected gaps in escalatory restraint. Also, the intrusive or covert employment or availability of AI-enabled surveillance, reconnaissance, or weapon systems could heighten

[7] 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/.

[8] Kathleen H. Hicks et al., *By Other Means Part 1: Campaigning in the Gray Zone* (Washington, D.C.: CSIS, 2019), https://www.csis.org/analysis/other-means-part-i-campaigning-gray-zone.

[9] Elias Groll, "How AI Could Destabilize Nuclear Deterrence," *Foreign Policy*, April 24, 2018, https://foreignpolicy.com/2018/04/24/how-ai-could-destabilize-nuclear-deterrence/. See Robert J. Bunker, *Terrorist and Insurgent Unmanned Aerial Vehicles: Use, Potentials, and Military Applications* (Carlisle, PA: Strategic Studies Institute and US Army War College Press, 2015); Zachary Kallenborn and Philipp C Bleek, "Swarming Destruction: Drone Swarms and Chemical, Biological, Radiological, and Nuclear Weapons," *Nonproliferation Review* 25, no. 5–6 (2018): 523–43; James Johnson, "Artificial Intelligence, Drone Swarming and Escalation Risks in Future Warfare," *The RUSI Journal* 165, no. 2 (2020): 26-36.

[10] J.R. Holmes, "Sea Changes: The Future of Nuclear Deterrence," *Bulletin of the Atomic Scientists* 72, no. 4 (2016): 228–233.

tensions and increase the chances of inadvertent escalation in a crisis, especially if the state being observed discovers, disables, or destroys a surveillance asset. AI will prove to be particularly problematic due to its precipitous technical progress and intersection with nuclear strategy. Countries such as Russia and China both appear to believe that the United States is trying to leverage AI to threaten the survivability of strategic nuclear forces, exacerbating mistrust that could be dangerous in a crisis.[11] As Paul Bracken observes, ongoing improvements in technology such as AI threaten to "undermine minimum deterrence strategies" and "blur the line between conventional and nuclear war" by dramatically improving the speed and effects of nonnuclear strike capabilities.[12]

For most of the nuclear age, the ability to characterize the operating environment, identify nuclear and conventional strategic attacks and discern real attacks from false alarms has been regarded as a benefit to crisis stability. By improving the accuracy and timeliness of warning, improving overall visibility and clarity on adversary actions, and increasing decision time, enhanced situational awareness and strategic warning seemed to reduce the risk of nuclear miscalculation and the use-it-or-lose-it pressures that could incentivize a nuclear first strike. In conventional conflicts, information dominance—much like air superiority—has been a fundamental component of precision warfare and a central feature of U.S. conventional military superiority in the post-Cold War period.[13] In the conventional arena, 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.[14]

***The United States has enjoyed the benefits of information dominance and the asymmetric advantage it offered. In other words, we could largely have our cake and eat it too. The question is, can we continue to do so?***

For the most part, the United States has enjoyed the benefits of information dominance and the asymmetric advantage it offered. In other words, we could largely have our cake and eat it too. The question is, can we continue to do so? Given the stakes involved, it is difficult to imagine that in a conflict between nuclear powers, adversaries could accurately discern U.S. intentions and allow such information dominance to proceed unchecked.

The days of clear delineations between nuclear and nonnuclear situational awareness capabilities—which help maintain a sharp firebreak between conventional and strategic conflict—seem limited at best. Future decision-makers may have to weigh the benefits of rapid, decisive military victory afforded by information dominance against the high-stakes risks of nuclear escalation.[15] To effectively manage crisis escalation, decision-makers 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 decision-making.

[11] Edward Geist and Andrew J. Lohn, *How Might Artificial Intelligence Affect the Risk of Nuclear War?* (Santa Monica, CA: RAND Corporation, 2018), https://www.rand.org/pubs/perspectives/PE296.html.

[12] P. Bracken, "The Intersection of Cyber and Nuclear War," The Strategy Bridge, blog post, January 17, 2017, https://thestrategybridge.org/the-bridge/2017/1/17/the-intersection-of-cyberand-nuclear-war.

[13] John A. Ardis and Shima D. Keene, *Maintaining Information Dominance in Complex Environments* (Carlisle, PA: U.S. Army War College, Strategic Studies Institute, October2018), https://publications.armywarcollege.edu/pubs/3658.pdf.

[14] Ibid.

[15] Hersman et al., *Under the Nuclear Shadow*.

This suggests we may need new tools, concepts, strategies, and policies to help guide us through this increasingly complex terrain. Of particular concern, as unpacked in our *On The Radar* project, 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.[16] 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*

Provocation pathways generally emerge from the inability to discern "defensive behavior" from actions that are more offensive in nature, including actions that could indicate first strike intentions or make second-strike options less secure. They often involve heightened risk-taking by either an observing or an observed state and perception dynamics associated with high-stakes security dilemmas—namely situations in which one party's efforts to lower perceive risks in turn raise risk perceptions for the competing state.[17]

For the observing state, such precise and time-sensitive situational awareness may create powerful first strike incentives—in part to prevent or preempt highly threatening actions by the observed state. For the observed state, such surveillance efforts may seem far more offensive than defensive in nature and therefore incentivize or justify a kinetic response, especially if the surveillance is intrusive in nature. Boundaries for these types of interactions and responses are very unclear. For the observed state: What is the adversary trying to detect or monitor, and why? Do they merely intend to observe? Is surveillance intrusive or beyond territorial limits? For the observing state: How should it consider counterattacks on surveillance assets? Does the type of attack matter? Non-kinetic? Tampering? Disablement? Spoofing? What are the thresholds and what constitutes an appropriate response? What role is there for transparency and risk reduction? If an adversary were to discover and target these surveillance systems, would such an attack be considered conventional or strategic?

This dynamic can be illustrated with an example scenario, such as the deployment of a HALE UAV over adversary territory. Consider this scenario: 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 an 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 because 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.

The inability of countries to delineate offensive and defensive intentions of capabilities that may directly challenge legal and political concepts of sovereignty could produce a spiraling sequence of actions and reactions, resulting in a loss of escalatory control along the conventional-nuclear seam.

[16] Ibid.

[17] John Baylis and Steve Smith, *The Globalization of World Politics: An Introduction to International Relations*, 3rd ed. (New York: Oxford University Press, 2005).

## Entanglement

Most research to date on this second pathway, entanglement—the commingling of conventional and nuclear forces, capabilities, or support systems—has focused on dual-use delivery systems capable of carrying both conventional and nuclear payloads, the integration of nuclear and conventional support structures such as command and control, and nonnuclear threats to nuclear weapons systems.[18] Far less work has been done on the informational aspects of conventional-nuclear entanglement and the implications for unexpected escalatory effects, especially with regard to situational awareness, surveillance, and warning capabilities.

We should expect states to have strong incentives to target command, control, warning, and surveillance systems early in a crisis to ensure conventional dominance, which will also threaten nuclear-related systems whether intentionally or unintentionally. But beyond this, we will need to wrestle with not just the dual-use nature of specific systems, but also the existence of an entirely comingled information ecosystem—warning, detection, surveillance, and targeting as well as the communications and decision support systems that support it—creating a highly networked, real-time, dual-use landscape that is both more precise and more complex across all levels of conflict—sub-conventional, conventional, and strategic.

The lack of distinction between the conventional and nuclear domains will only intensify as new surveillance and warning systems come online. Consider the case of the North Warning System (NWS) which is reaching the end of its service life. NWS is comprised of 11 long-range and 36 short-range missile warning radars operated by the United States and Canada under the auspices of the North American Aerospace Defense Command (NORAD). NORAD must select a notional successor early warning system by 2021 so that it is operational by the mid-2030s.[19] Some call for all-domain awareness (through new sensors capable of dual-use data and information collection in multiple domains including land, space, maritime, subsurface, and aerospace) and action, requiring dual-use technology.[20] Furthermore, some have called for the integration of advanced machine learning and other techniques to better anticipate or predict inbound threats.[21] Ostensibly, such an approach could expand decision time and open response windows earlier. What is not clear, however, is how such a transformation of our homeland early warning systems might undermine targeting disincentives of warning systems or exacerbate first-mover incentives in escalatory ways.

## Information Complexity

The final pathway involves escalation through information complexity. Escalation through information complexity results from decision-makers' inability to seek, manage, and interpret information effectively. Emerging technologies for strategic situational awareness have the potential to fundamentally transform the information domain and, if used effectively, to help decision-makers manage crises more effectively with lower levels of risk. The U.S. Air Force has defined this new information environment by four "Vs"—greater volume (collection of

[18] James M. Acton, "Escalation through Entanglement: How the Vulnerability of Command-and-Control Systems Raises the Risks of an Inadvertent Nuclear War," *International Security* 43, no. 1 (Summer 2018): 56–99, https://doi.org/10.1162/isec_a_00320; James M. Acton, *Is It a Nuke?: Pre-Launch Ambiguity and Inadvertent Escalation* (Washington, D.C.: Carnegie Endowment for International Peace, 2020), https://carnegieendowment.org/2020/04/09/is-it-nuke-pre-launch-ambiguity-and-inadvertent-escalation-pub-81446.

[19] Ernie Regehr, *Replacing the North Warning System: Strategic competition or Arctic confidence building?* (Vancouver: The Simons Foundation, 2018), http://www.thesimonsfoundation.ca/highlights/replacing-north-warning-system-strategic-competition-or-arctic-confidence-building.

[20] Andrea Charron, "Beyond the North Warning System," *War on the Rocks*, September 7, 2020, https://warontherocks.com/2020/09/beyond-the-north-warning-system/.

[21] Theresa Hitchens, "The Key To All-Domain Warfare Is 'Predictive Analysis:' Gen. O'Shaughnessy," Breaking Defense, May 5, 2020, https://breakingdefense.com/2020/05/the-key-to-all-domain-warfare-is-predictive-analysis-gen-oshaughnessy/.

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).[22] 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.[23]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.

To evaluate some of the risk assessments identified in research and to explore the decision-making process of policymakers and technical experts in the throes of crises under a nuclear shadow, the Project on Nuclear Issues developed and conducted a series of tabletop exercises on two fictitious regional scenarios. Through these exercises, it was evident that the precise, rapid, and persistent information that will be made available through emerging technologies is only as good as the decision-making process it supports. 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. Excessive caution may avoid unnecessary provocation. It may also force decision-makers 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.

Faulty decision-making may 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. This suggests that psychology, particularly in the form of pre-held beliefs and cognitive biases, is underappreciated when examining the relationship between crisis decision-making 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, as well as properly grasp their benefits and limitations.

***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.***

Further, technologists and operators accustomed to a conventional-only battlefield, where information dominance and precision warfare are prioritized, may not fully appreciate the concerns of decision-makers when such a crisis or conflict occurs under a nuclear shadow. From a nuclear decision-making standpoint, almost any action, including those designed to enhance situational awareness, will be viewed and construed through the lenses of signaling, perceived provocation, and escalation management.

[22] Shane P. Hamilton and Michael P. 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.
[23] 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.

## Takeaways and Recommendations

In this environment, there is no realistic path to "disentanglement" of the nuclear and conventional components of warning and ISR or the dumbing down of information and situational awareness. Firebreaking, and the "escalation ladder"-based thinking on which the concept depends, may be a relic of the past. Many technologies (e.g., AI, advanced sensors, and 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 appropriately. Understanding failure modes and improving risk-benefit assessments of emerging technologies, especially in terms of artificial intelligence and machine learning is critical. Future nuclear and conventional missions will be distinguished less by the capabilities used and more by the missions to which they are assigned. Thus, risk reduction approaches that emphasize resiliency, redundancy, and transparency may prove more fruitful both operationally and in terms of their stabilizing value.

This will require a better-shared understanding of triggers and thresholds for escalation across the information and situational awareness space along the conventional strategic seam. This should be a focus area for conventional-nuclear integration planning, exercising, and capability development. The strategic SA ecosystem may be combined across the conventional and nuclear realms, but so far, 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 are essential to understanding the trade-offs, risks, and benefits of conventional-nuclear integration in the strategic SA arena.

In addition, there needs to be a careful reexamination of how we build, explain, and manage warning systems of the future. There will be a need to carefully consider the application of predictive systems for strategic warning. As mentioned earlier, NORAD renewal might also place a greater emphasis on predictive analysis to manage multi-domain conflict rather than relying on "traditional stovepiped systems."[24] This may be right and even inevitable, but we need accompanying tools to inform and communicate associated escalation risks.

The divide between technology and policy regarding the benefits, risks, and requirements for strategic situational awareness capabilities has to be bridged. Information complexity and a lack of familiarity with strategic surveillance and warning capabilities introduce 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. Moreover, we can expect that decision-makers will bring high levels of escalation anxiety to any crisis between nuclear-armed adversaries. 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. As Admiral James Alexander "Sandy" Winnefeld, Jr. argued earlier this year, "there should be a virtuous cycle between ways (i.e. the strategic and operational concepts we use to accomplish our ends) and means (i.e. the things we buy to breathe life into those concepts)"—or constant dialogue between technologists and strategists.[25]

Finally, arms control—as both a component of and contributor to strategic stability—needs to be broader than nuclear. Establishing better risk reduction-oriented "rules of the road" for cyber, space, and digital communications systems architectures—especially AI-enabled—will be increasingly important as nuclear-armed states seek ways to

[24] Hitchens, "The Key To All-Domain Warfare."

[25] Winnefeld, James Alexander. Other. *Technology, Strategy, and the Future of Policy*, August 2020.

dampen escalatory pressures across this complex technological landscape in the absence of more traditional firebreaks. Figuring out the implications of these technologies for arms control and creating effective mechanisms—or using existing treaties—for their control will be an important and mammoth undertaking.[26]

Regardless, doctrinaire or traditional nuclear-focused approaches to deterrence and arms control—from declaratory policy to numerical arms reduction treaties—are unlikely to meet the escalatory challenges raised by today's surveillance and warning capabilities and their application to future warfare. Rather, such a challenge can only be met through effective integration, collaboration, and education across nuclear and conventional components of the national security enterprise.

## AUTHORS

***Rebecca K.C. Hersman*** *is director of the Project on Nuclear Issues and senior adviser in the International Security Program at the Center for Strategic and International Studies (CSIS).* ***Reja Younis*** *is a program manager and research associate with the Project on Nuclear Issues in the International Security Program at CSIS.*

## ABOUT CSIS

*Established in Washington, D.C., over 50 years ago, the Center for Strategic and International Studies (CSIS) is a bipartisan, nonprofit policy research organization dedicated to providing strategic in-sights and policy solutions to help decisionmakers chart a course toward a better world.*

*In late 2015, Thomas J. Pritzker was named chairman of the CSIS Board of Trustees. Mr. Pritzker succeeded former U.S. senator Sam Nunn (D-GA), who chaired the CSIS Board of Trustees from 1999 to 2015. CSIS is led by John J. Hamre, who has served as president and chief executive officer since 2000.*

*Founded in 1962 by David M. Abshire and Admiral Arleigh Burke, CSIS is one of the world's preeminent international policy institutions focused on defense and security; regional study; and transnational challenges ranging from energy and trade to global development and economic integration. For eight consecutive years, CSIS has been named the world's number one think tank for defense and national security by the University of Pennsylvania's "Go To Think Tank Index."*

*The Center's over 220 full-time staff and large network of affiliated scholars conduct research and analysis and develop policy initiatives that look to the future and anticipate change. CSIS is regularly called upon by Congress, the executive branch, the media, and others to explain the day's events and offer bipartisan recommendations to improve U.S. strategy.*

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

[26] Michael T. Klare, "The Challenges of Emerging Technologies," Arms Control Association, December 2018, https://www.armscontrol.org/act/2018-12/features/challenges-emerging-technologies.