SEPTEMBER 2021

The Adversary Gets a Vote

Advanced Situational Awareness and Implications for Integrated Deterrence in an Era of Great Power Competition

Rebecca K.C. Hersman and Reja Younis

Calls for information dominance and decision superiority, especially across U.S. homeland-defense and strategic-warning systems, have taken on renewed urgency as the security environment grows more complex and competitive. In April 2021, General Glen VanHerck, commander of the North American Aerospace Defense Command (NORAD) and the U.S. Northern Command (USNORTHCOM), stated to the House Armed Services Committee, "I believe our future success in USNORTHCOM, our fellow U.S. combatant commands, and NORAD requires all-domain awareness, information dominance, and decision superiority. Our competitors have invested heavily in weapons systems that can be launched against distant targets with little to no warning, as well as stealthy delivery platforms specifically designed to evade detection by existing sensors." Undergirding this push is a growing confidence that new technologies—including advanced sensing, quantum computing, machine learning, and advanced data management, among others—can deliver the information dominance needed to outrun and outgun a conventional or strategic attack by providing a situational awareness picture that is far more useful than the warning systems of the past.

Seeking to prove the efficacy of this approach, in July 2021 USNORTHCOM conducted the Global Information Dominance Experiments (GIDE), which combined global sensor networks, artificial intelligence (AI) systems, and cloud computing resources to "achieve information dominance" and "decision-making superiority." According to General VenHerck, using this AI-enabled platform for rapid data collection and integration could allow for more proactive forecasting and expand the decision time available to commanders in high-stress scenarios. Such predictive capabilities could be transformative, shifting the United States from a reactive footing to a far more preventive one.

The many benefits of informational superiority are obvious—including more precise warning, expanded decision time, and improved response options. Moreover, much of the U.S. strategic warning architecture is

in desperate need of overhaul. The North Warning System, for instance, comprises a series of unmanned, long- and short-range radars in Greenland and the North American Arctic in support of air defense and frontier control but is reaching the end of its serviceable life. It is furthermore threatened by climate change and not tailored for emerging risks such as hypersonic gliders, which—with the speed of ballistic missiles and the maneuverability of cruise missiles—could fly around it.

Yet security dilemma dynamics and escalatory risks are inevitable when large asymmetries in military capabilities emerge under a nuclear shadow. The pursuit of superiority—informational, decisional, or any other form—is inherently a drive for asymmetric advantage. As the Department of Defense (DoD) further develops integrated deterrence as its overarching strategic concept, it will become increasingly important to appreciate the stability risks and benefits associated with emerging intelligence, surveillance, and reconnaissance (ISR) capabilities, from both an arms-race and crisis-management perspective.

For decades, stable nuclear deterrence has rested on the secure second-strike principle—the ability of a nuclear-armed state to withstand a nuclear attack and still launch a counterstrike of devastating proportion. But stable deterrence has also relied upon an equally important, if less often emphasized, corollary: the absence of first-strike incentives that would drive a country to move either in anticipation of an attack or in reaction to an adversary's perceived overwhelming strategic advantage. For most nuclear-armed states—and certainly for the United States, Russia, and China—stable deterrence depends not only on the size and characteristics of their nuclear arsenals, but also on the ability to hide significant portions of that arsenal from adversaries' prying eyes and protect their secure second-strike capabilities, at least in part, under a veil of opacity.

As the Department of Defense (DoD) further develops integrated deterrence as its overarching strategic concept, it will become increasingly important to appreciate the stability risks and benefits associated with emerging intelligence, surveillance, and reconnaissance (ISR) capabilities, from both an arms-race and crisis-management perspective.

Can the United States lead, dominate, and win this information race? Perhaps. But doing so may invite greater risk of an arms race and deterrence failure than some seem ready to acknowledge or prepare for. Furthermore, the argument for "deterrence by detection"—the idea that extensive peacetime use of unmanned aircraft systems (UAS) for surveillance may help "deter" conventional acts of aggression by China or Russia (as put forward by Thomas Mahnken, Travis Sharp, and Grace Kim in April 2020 and underscored by Marine Corps Commandant General David Berger in September 2021)—puts another spin on this challenge. If such persistent capabilities deliberately or inadvertently detect and observe strategic assets, an adversary may believe that its nuclear arsenal is at risk, potentially escalating a crisis. In addition, many assets associated with persistent information dominance or "deterrence by detection" are highly vulnerable to attack or disruption. Before embarking on such an approach, it is essential to have a better understanding of the escalatory risks and responses to this form of deterrence failure in which an adversary attacks, evades, or ignores such capabilities.

As DoD embarks on a new national defense strategy—rooted in the concept of integrated deterrence of war and conflict with nuclear-armed, peer and near-peer competitors such as Russia and China—a singular focus on integration is insufficient. Rather, equal (or more) attention should be given to the ways in which deterrence concepts such as "stability" and "ambiguity" interact with a conventional lexicon focused on "superiority" and "dominance," especially when considering capabilities such as early warning, situational awareness, and ISR that straddle the conventional and strategic arenas. The first section of this paper scopes advanced situational awareness technologies that could fuel first-strike incentives and erode secure second-strike capabilities. The next unpacks Russian and Chinese advancements and arms racing in this area. This is followed by an exploration of the way forward in an era of strategic competition and implications for an integrated, deterrence-based strategy.

Photo: Chief Petty Officer Shannon Renfroe/U.S. Navy

Erosion of Stable Nuclear Deterrence and Reactionary Arms Racing: The Price to Pay for Advanced Situational Awareness?

Capabilities to monitor activities associated with nuclear weapons can prove highly stabilizing by confirming assurances of non-aggressive intent, providing verifiable transparency, and reducing risk of strategic surprise. Yet mobility and opacity—the "**hiding**" of nuclear forces—also play a critical role in stable deterrence by maintaining confidence in a secure second strike. As the precision, persistence, and coverage of surveillance technology continues to improve, perceptions of survivability may decline, especially as strategic and conventional systems become more integrated. First, as conventional situational-awareness 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. For example, the MQ-9B SkyGuardian remotely piloted aircraft—with its multi-domain, multi-role applications, including for maritime warfare—may have originally been intended for contingency and conventional wartime operations. However, it could also track a smaller country's nuclear mobile missiles or surveil for other warning indicators, such as garrison movements, changes in everyday routines, or the buildup of forces. As these capabilities become more advanced and operate at longer standoff ranges, they might also be useful in tracking Russian or Chinese strategic assets. For example, constellations of smallsats or nanosatellites, such as CubeSats, could allow for real-time, continuous, high-definition visual and infrared imaging of areas of interest. In conjunction with airpower, cruise missiles, and other conventional strike assets, such high-fidelity surveillance capabilities may enable operators to locate and engage a formidable range of targets.

In addition, while not imminent, advancements in submarine-detection technologies—including commercial satellite imagery, synthetic-aperture radar (SAR), and hydro-acoustic sensors—could ultimately undermine the most survivable nuclear-weapons delivery platforms. What is more, non-acoustic submarine-detection technologies—those that do not rely on the collection of soundwaves emitted or reflected by a submerged vehicle for location—may support future capabilities to track both an adversary's conventional-only attack submarines as well as nuclear-armed ballistic-missile submarines (SSBNs). Using light-based imaging (such as lidar) or magnetic anomaly detectors (MADs), 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. If SSBNs were identified during a crisis using such detection methods, a surveilled state might view the sea leg of its nuclear deterrent to be compromised, potentially leading to escalation.

> ***Capabilities to monitor activities associated with nuclear weapons can prove highly stabilizing by confirming assurances of non-aggressive intent, providing verifiable transparency, and reducing risk of strategic surprise. Yet mobility and opacity—the "hiding" of nuclear forces—also play a critical role in stable deterrence by maintaining confidence in a secure second strike.***

Thus, for the targeted state, adversaries' ability to inform or enable preemptive or preventive action may make it increasingly challenging to conceal nuclear forces effectively. In such cases, the actual or perceived ability of the more technologically advanced country to carry out precision-strike missions against strategic nuclear assets could make any information dominance—even if purely defensive and/or conventional 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. ISR assets in its airspace were a threat to its nuclear assets regardless of their actual assigned mission. Hence, highly intrusive surveillance assets could undermine stable deterrence by creating pressure for a state to posture its forces for early use in a crisis before its nuclear option is curtailed. In other cases, advanced surveillance may trigger other competitive dynamics, such as arms racing, either in terms of expanding and diversifying strategic assets or increasing countersurveillance capabilities in hopes of holding U.S. strategic assets at risk.

These dynamics will be further complicated by the increasing interdependence of systems designed to support both nuclear and conventional missions—a trend that may be largely irreversible, particularly in the areas of strategic warning and surveillance and command, control, and communications. While the concepts and tools of nuclear warfare (including command, control, and communications and detection, warning, and situational-awareness capabilities) used to be distinct and highly compartmentalized from those designed to support conventional warfighting, today they are no longer. In fact, the expansion of dual-capable delivery systems and the diversification of strategic forms of warfare to include sub-conventional, cyber, space-based, and advanced high-precision conventional strike capabilities have sharply eroded the structural firebreaks between strategic and conventional capabilities that have characterized much of the nuclear age.

Even as modernized NC3 systems seek to ensure a "thin line" of capability reserved exclusively to support nuclear missions under extreme circumstances, most nuclear and conventional missions will continue to rely on shared or dual-use capabilities for situational awareness, warning, and communications. For instance, conventional missile-warning systems currently depend on dual-use surveillance capabilities, increasing the risk that an attack on these systems during a conventional conflict, for conventional purposes, could have profound strategic implications. Advanced, long-range, and often dual-capable missile systems such as hypersonic weapons—both hypersonic glide vehicles and hypersonic cruise missiles, as well as long-range traditional cruise missiles and other capabilities, are designed to elude traditional U.S. early-warning systems—have proliferated dramatically in recent decades, including among a range of nuclear-armed adversaries (such as China, which has recently developed the DF-26 IRBM). Accordingly, these systems' reliance on comprehensive and integrated warning systems now needs to figure significantly in the planning and execution of conventional conflicts. These systems are also no longer as physically "firewalled" as conventional and nuclear systems were in the past, including for strategic warning and communications that might counter or disrupt escalatory pressures. This is significant because 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.

Even missile-defense capabilities could be viewed 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 targeting North Korea's short-range ballistic missiles using interceptors with a range of 200 kilometers (124 miles). However, public statements suggest Beijing is concerned about potential uses of the AN/TPY-2 radar deployed with THAAD, fearing it could be used to gather information about China's missile tests (both conventional and nuclear-capable) and other military operations, thus weakening the credibility of China's nuclear deterrent. If an adversary felt threatened during a crisis and targeted such systems, would such an attack be considered conventional or strategic in intent and implication?

Evolving technology has also made space-based surveillance systems more vulnerable to a range of disruptive capabilities, including electronic warfare (e.g., spoofing and jamming), blinding, disabling, and kinetic ground-based anti-satellite weapons. In addition, the conventional missions of space-based assets suggest they could be seen as fair game for targeting during a conventional crisis or conflict. 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 situational awareness. In a similar vein, the Space Tracking and Surveillance System (STSS), developed and operated by the Missile Defense Agency, detects and tracks ballistic missiles through all

phases of their flight and transmits and provides data to radars. Over the course of a conventional conflict between the United States and an adversary with anti-satellite capabilities, disruptions of dual-use satellites that provide early-warning functions would risk 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 acting 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 detect any intercontinental ballistic missiles (ICBMs) China launches against the United States.

Finally, given the strategic advantage that would be conferred by the global information-dominance system GIDE envisioned, how would the United States react to any attempt to disrupt, disable, or destroy such a system? Traditionally, military planners have assumed that nuclear command and control assets would be "off limits" in a conventional crisis because of the highly escalatory significance of such an attack. But there are no formalized codes of conduct or agreed boundaries surrounding such assumptions, and it remains unclear how they would apply across such a large and dual-use information architecture.

How Do Defining Features of Emerging Situational-Awareness Capabilities Affect Adversarial Behavior?

There are potentially stabilizing benefits to the U.S. push for decision superiority and the transformation of the situational awareness ecosystem in terms of reducing risks of miscalculation, misinterpretation, and overreaction to adversary actions. However, in a contested security environment with peer and near-peer competitors, such advantages impose costs on potential adversaries that will not go unanswered, particularly if the persistent nature of U.S. strategic situational awareness and missile defense capabilities undermine the perceived survivability of an adversary's nuclear force. We can and should expect that these countries will expand their forces numerically as with China, invest in capabilities that elude surveillance as with Russia, and expand countersurveillance capabilities as we see with both China and Russia, especially in their increasingly aggressive space postures. Russia and China will not leave the United States to unchecked technological dominance, even if those efforts are characterized as non-kinetic and defensive. Rather, increased arms racing across a range of platforms, domains, and technologies may prove inevitable as the fielding of new capabilities continues to expand. In crisis, these dynamics could be equally or more worrisome, especially given that any conflict with Russia or China (even if intended to remain well below the nuclear threshold) will inevitably involve a full range of highly advanced strategic capabilities that operate along the conventional-nuclear interface.

China's burgeoning nuclear force—which is increasing its arsenal and expanding to a triad of delivery systems—suggests perceived **vulnerabilities** vis-à-vis the United States' missile defense (particularly THAAD, Aegis, and radars), technological ISR edge, and conventional precision-strike systems. Unclassified sources now indicate dramatic **developments** in Chinese ICBM capability—including the **DF31A** missile and the discovery of new silo fields, possibly for DF41s. In addition, China's ground-based missile forces are operated by the People's Liberation Army Rocket Force, which commands nuclear, conventional, and dual-use missile systems, all of which could be entangled in several ways.[1] Furthermore, China's

1 Whether Chinese entanglement of nuclear and conventional forces is intentional or inadvertent, rising scholars such as David Logan highlight the risk of misunderstandings between China and the United States, **arguing** that if U.S. officials believe China's entanglement is both extensive and deliberate, they may be more inclined to take riskier military operations under the assumption that China has considered and prepared for the associated risks. Alternatively, if Chinese officials have not considered those risks, they are likely to be less prepared for the risks of escalation and may be more likely to interpret ambiguous U.S. actions in the worst possible light.

development of a range of technologies and tools for its nuclear forces—including maneuverable reentry vehicles (MARVs), multiple independently targetable reentry vehicles (MIRVs), hypersonic glide vehicles, decoys, chaff, jamming, and thermal shielding—appear designed to counter other countries' ballistic-missile defense, ISR, and precision-strike systems. China is also bolstering its sea deterrent with **Type 094 Jin-class** nuclear-powered SSBNs—which may **not** be on par with other leading navies but could still potentially hold some U.S. assets and territories at risk.

Moreover, China seeks similar capabilities to the United States to match it as a strategic competitor. Despite its public **stance** against the weaponization of space, China **continues** to strengthen its military space capabilities, particularly in space-based ISR, satellite communications, and satellite navigation. China also continues to modernize its command, control, communications, computers, and intelligence (C4I) to enable rapid information sharing and decisionmaking. The People's Liberation Army will likely continue to focus on fighting and winning the information race by **implementing** emerging technologies such as big data, AI, and cloud computing to provide reliable, automated platforms that yield further process efficiencies.

Meanwhile, Russia is reinforcing its anti-access/area denial (A2/AD) posture—**emphasizing** electronic warfare and other information-warfare capabilities, incorporating denial and deception as part of its approach—while developing hypersonic and dual-capable delivery systems (such as **Avangard**, Kinzhal, and Tsirkon) specifically designed to evade U.S. warning and defense systems. The primary catalyst behind these developments also appears to be fear regarding U.S. missile-defense and ISR capabilities. In fact, in 2018, President Vladimir Putin **stated** that the development of these weapons was directly due to the U.S. withdrawal from the Anti-Ballistic Missile Treaty in 2002. Russia also seeks to **improve** its C4I and ISR capabilities to enable better targeting and more timely responses to perceived threats.

Finally, future confrontations with Russia or China will not necessarily resemble traditional warfare. On the contrary, as actors seize upon technological advancements, conflict is more likely to occur in the "gray zone" below conventional conflict and beyond traditional statecraft. China's **gray-zone** actions include military intimidation, paramilitary activities, information operations, industrial and academic espionage, and economic coercion. Russia is also an involved player in the gray zone, liable to employ military intimidation, weaponize social media, conduct information and cyber warfare, and fund proxy groups and political organizations hostile to Western institutions. Such sub-conventional tactics pose unprecedented **risks** to crisis stability, placing new and different demands on surveillance and warning systems. And as the nature of conflict shifts, pathways to escalation may be far less easily understood or defined. As a result of emerging technologies and a new, highly contested gray zone of strategic competition, future conflicts may be better characterized by "**wormhole escalation**"—a non-linear pathway characterized by disinformation, weaponized social media, and the blurring of lines between conventional/nuclear capabilities and conventional/strategic conflict. "**Wormholes**" may pierce though the fabric of deterrence and allow competing states to inadvertently and suddenly traverse between sub-conventional and strategic levels of conflict in accelerated and decidedly non-linear ways.

The Way Forward in an Era of Strategic Competition: Implications for an Integrated Deterrence-Based Strategy

When considering the complex, high-tech nature of operations along the conventional–nuclear interface—including their potential to directly impact the United States—the U.S. government needs to untangle some of the escalatory, arms-racing implications of information dominance and decisional superiority,

as well as what this can mean in a conflict with nuclear-escalation potential. Will the race for such capabilities ultimately degrade the stealth and opacity of sea-based assets that currently underpin credible deterrence? How can the United States and its adversaries untangle and protect strategic assets from counterforce targeting that could overly incentivize a first strike? Will the United States necessarily lead, dominate, and win this information race? And, above all, will winning be worth the cost?

Moving forward, the United States needs to be judicious in determining the semantics and applications of concepts such as "information superiority" and "decision dominance." An unbridled pursuit of superiority and dominance will inevitably prompt a competitive response and taken too far, could undermine rather than reinforce stable deterrence. Moving to an overall integrated deterrence posture will require some careful recalibration of posture and communications in this arena. Establishing better risk-reduction oriented "rules of the road" for cyber, space, and digital-communications systems architectures will be increasingly important as nuclear-armed states seek ways to 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—to manage them will be an important and complex undertaking.

Moving forward, the United States needs to be judicious in determining the semantics and applications of concepts such as "information superiority" and "decision dominance." An unbridled pursuit of superiority and dominance will inevitably prompt a competitive response and taken too far, could undermine rather than reinforce stable deterrence.

Strategic dialogue and engagement across the information domain will also be critical. As evidenced above, there is a notable **perceptions gap** in ISR technologies between the United States and China that cannot be resolved if Washington and Beijing continue to talk past each other. Issues of escalatory risks associated with warning, surveillance, and information should be included in any security and stability dialogues with adversaries. Such dialogues might also consider the possibility of instituting constraints or other measures to discourage the risky surveillance of strategic assets. Furthermore, some strategic surveillance could be designated off limits for attack, disablement, or disruption. In other words, adversaries could recognize that persistent surveillance is a mutual interest that favors all parties. The United States could also seek opportunities for "shared" situational awareness with Russia and China that might offer transparency and accountability. Strategic situational awareness capabilities and the information they provide need to be made more adaptable and flexible to potential requirements for enhanced transparency, signaling, self-attribution, information sharing, and public disclosures. This may involve developing mechanisms, protocols, and options to manage collection assets beyond traditional covert, clandestine, or intelligence-oriented concepts of operation—which can be used for signaling and crisis management during a conflict with a nuclear-armed adversary.

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 these technologies appropriately. It will be critical to understand failure modes and improve risk–benefit assessments of emerging technologies, especially in terms of artificial intelligence and machine learning. 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 in the information and situational awareness space, especially along the conventional–nuclear seam. This should be a focus area for conventional nuclear-integration planning, exercises, and capability development. The strategic situational awareness ecosystem may straddle the conventional and nuclear realms, but (so far) the communities responsible for planning, policy, and crisis management in these two operational areas do not. That needs to change. Communication and collaboration across both communities are essential to understanding the tradeoffs, risks, and benefits of conventional–nuclear integration in the strategic situational awareness arena.

In addition, there needs to be a careful reexamination of how to build, explain, and manage warning systems of the future, as well as the application of predictive systems for strategic warning. The lack of distinction between the conventional and nuclear domains will only intensify as new surveillance and warning systems come online. For example, renewing NORAD might also place a greater emphasis on using predictive analysis to manage multidomain conflict rather than on "traditional stovepiped systems." This may be right and even inevitable, but the United States needs accompanying tools to inform and communicate associated risks regarding arms racing and crisis management.

Finally, these issues cannot solely be addressed as matters of capability, posture, and doctrine. Rather, it is critical to study and implement best practices for the interactions between these information systems and the decisionmakers who will be responsible for interpreting and acting upon the information provided. Placed in a novel unfolding crisis with novel capabilities, policymakers may trust technologies too much or too little and may rely on cognitive biases or preconceived value judgments, particularly in terms of the escalation risk associated with a nuclear shadow. The divide between technology and policy regarding the benefits, risks, and requirements for strategic situational awareness capabilities will need to be bridged. It will be vital to train, socialize, and prepare decisionmakers regarding emerging technologies in a pre-crisis setting. Improved familiarity with emerging technologies may reduce escalatory risks and improve decisionmaking and crisis response when it matters most.

Information and decisionmaking architectures need to be modernized and expanded to account for a rapidly evolving technical landscape and increasingly competitive security environment. Yet while the United States should seek to maintain a competitive advantage in the information realm, superiority and dominance—let alone a reimagining of deterrence based upon these principles—are unrealistic objectives that may risk escalation and strategic instability. Bottom line? Proceed with caution: speed bumps and blind corners ahead. ■

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.*

This report is made possible by support from General Atomics and general support to CSIS.