Airman with 321st Contingency Response Squadron security team patrols with Ghost Robotics Vision 60 prototype at simulated austere base during Advanced Battle Management System exercise on Nellis Air Force Base, Nevada, September 3, 2020 (U.S. Air Force/Zachary Rufus)

Deter in Competition, Deescalate in Crisis, and Defeat in Conflict

By Glen D. VanHerck

The North American Aerospace Defense Command (NORAD) and U.S. Northern Command (USNORTHCOM), both located in Colorado Springs, Colorado, are two distinct commands, bound together and united in a common purpose—charged with the resolute mission of defending North America. NORAD defends the United States and Canada against threats in the air domain and provides aerospace and maritime warning. Founded in 2002 in the wake of 9/11, USNORTHCOM defends the United States against threats across all domains, conducts cooperative defense activities with our allies and partners in North America, and, when required, supports Federal, state, and local agencies with unique military capabilities to conduct defense support of civil authorities.

General Glen D. VanHerck, USAF, is Commander of U.S. Northern Command and North American Aerospace Defense Command.

Global Competition

Today, NORAD's and USNORTHCOM's missions continue to use a multitude of sensors including the 1980s North Warning System, our network of globally positioned ballistic missile defense radars, and the Integrated Undersea Surveillance System. As the world's security environment has evolved over time, our legacy systems have become increasingly challenged, even as our attention drifted away from the possibility of major conflict, especially the possibility of conflict in North America.

Since August 1990, when Iraq invaded Kuwait, our national focus has been centered on the Middle East through operations *Desert Storm*, *Iraqi Freedom*, and *Enduring Freedom*. Meanwhile, our competitors' capabilities have advanced. Over this three-decade period, the United States developed strategies, plans, and capabilities focused on projecting power forward in order to take the fight to rogue regimes, violent extremist organizations, and other potential adversaries. This led to a tendency toward tactical thinking against individual actors, rather than the strategic thinking and analysis necessary to confront and compete with peer competitors. It instilled a preference for kinetic solutions over other options—including deterrence and an acquisition strategy that favored systems (often expensive) to confront single threats in one domain over multithreat, multidomain systems. These right-of-launch response plans, rather than left-of-launch denial and deterrence efforts, constrained our actions and decisionmaking.

Meanwhile, our competitors took this limitation as an opportunity to develop and advance capabilities that are specifically aimed at perceived seams in our homeland defenses and through a framework of constant global competition. Russia has developed a military doctrine that envisions nonnuclear strikes on an adversary's critical infrastructure to compel termination of an escalating conflict, and it has repeatedly demonstrated its ability to hold our homeland at risk through heavy bomber patrols near North America. Following one such patrol in December 2018, official Russian press highlighted that these flights could "pose a serious threat for the most important strategic facilities on U.S. territory." China, too, has developed a robust ability to threaten our critical infrastructure in the cyber domain and will likely field capabilities to do so with conventionally armed cruise missiles in the next 5 years. While China's intent for these capabilities is less clear, we suspect Beijing would use them to deter and frustrate our force flows across the Pacific in the event of a regional conflict. Finally, Vladimir Putin's *Strategy for Developing the Russian Arctic Zone and Ensuring National Security Until 2035* and the Chinese government's declaration of being a "near-Arctic state" are powerful indicators of their intent to exert influence in that region. Both competitors have pursued their efforts with national-level investments and a singular purpose: to compete with the United States in every domain.

In addition to our peer competitors, the United States continues to face threats from rogue regimes, such as Iran and North Korea, that attempt to hold the Nation at risk through proxies, cyber warfare, North Korea's nuclear weapons program, and advancements in missile technology.

We also face threats across the globe from corruption and poor governance engendered by transnational criminal organizations (TCOs), which are creating opportunities for economic competition, influence operations, and exploitation by our competitors—the very definition of unrestricted warfare. The destabilizing effects of TCOs can be seen at our border, in our cities, and even in our homes. Drug cartels have evolved past their traditional model of smuggling cocaine into the United States and have transitioned to moving precursor materials and guns to the south, fueling the flow of synthetic drugs into the United States as well as increasing instability south of the border. Cartel arsenals are competitive with our partners' law enforcement organizations and militaries, further challenging the legitimate monopoly of the state on the use of force.

Global competitors are confronting the United States from all directions and in all domains. These developments challenge our legacy warning and assessment systems. The stakes to defend the homeland are higher now than they have been in decades—and for NORAD and USNORTHCOM failure is not an option.

In this particular strategic security environment, it is imperative that we evolve our capabilities, force structures, authorities, and culture to confront the reality of constant global competition. We must embrace a comprehensive perspective to address these threats, develop a robust and inclusive information-sharing ethos, modify homeland defense policy, and demand that we go faster in all aspects of planning, force design, force management, acquisitions, and budgetary policy. Through this approach, we can and will deter our competitors in competition, deescalate in crisis, and deny or defeat in conflict.

Global Perspective Lens

Our competitors' actions are *global*, not regional. We must match this reality; we cannot continue to apply a regional perspective to plans, force management and design, or a parochial approach to acquisitions. Regionally focused plans do not address the fact that our peer competitors or potential adversaries are not constrained by our organizational boundaries or our command and control. They are capable of exploiting one theater's crisis and flanking the United States in another, bypassing our surge layer of fielded forces to strike at the homeland and compromise our ability to reinforce when and where needed. Based on this capability, the current notion espoused in U.S. doctrine of a single supported commander, with all others supporting, is impracticable. Because potential adversaries' actions will likely be global, every combatant commander may simultaneously be both a supported—and supporting—commander. We must create global plans that have regional components, focused on strategies, plans, force management, and force design and development concepts that integrate homeland defense and strategic deterrence into every aspect of our defense, from planning to execution.

But current operational plans do not accomplish this goal. Generically, our OPLANs double- or even triple-task forces and resources, creating a competition for high-demand, low-density assets. That means, for example, in a crisis overseas, the Secretary of Defense, with advice from the Chairman as the Department of Defense (DOD) global integrator, will have to adjudicate competing requirements from multiple combatant commands to determine apportionment

USS *Connecticut* surfaces in support of Ice Exercise 2018, Beaufort Sea, March 10, 2018 (U.S. Navy/Micheal H. Lee)

of scarce resources—compromising response and, more importantly, ceding valuable and irreplaceable time to the adversary. OPLANs today need to move past this model, identify distinct requirements for each commander, and deconflict force apportionment in advance, knowing that simultaneous demands will exist in any large-scale crisis.

From a capabilities standpoint, we treat the homeland differently than other theaters. Because the homeland was a relative sanctuary for more than 30 years after the fall of the Berlin Wall, NORAD and USNORTHCOM forces have been trained and configured for day-to-day and steady-state operations, not for the possibility of conflict in the homeland. Today, we do not have a persistent capability to generate high-tempo sustained operations within the United States and Canada in response to crisis, and we have not routinely equipped or trained our continental-based forces to operate in all environments, especially the Arctic. Likewise, our air operations centers (AOCs) in the homeland possess a fraction of the personnel and capabilities of AOCs supporting other combatant commands. North America will likely be a theater of operations in any future peer fight. We must regain the ability and mindset to be ready to fight tonight. Because our requirement is not to be ready for day-to-day operations—but to be prepared for crisis every day.

The good news is that the transition has begun. We are modifying our tactics, techniques, and procedures and renewing commitment to exercising our forces against worst-case scenarios. As an example, multinational polar exercises such as Arctic Edge, Northern Edge, and ICEX are increasing our readiness and presence in the Arctic, and we are conducting increasingly complex national-level exercises to engage in global competition.

If our competitors believe that they can destroy our will or ability to surge forces from the United States because of a perceived inability to defeat their attacks, they will be emboldened to aggressively pursue their strategic interests. In essence, this situation creates an opportunistic gap between our nuclear strategic deterrent and conventional deterrent capability for potential adversaries to exploit. This opportunity creates intent and, perversely, an incentive for adversary action. Put more boldly, a strategy that assumes unfettered power projection, given the current strategic environment, is *a losing strategy*.

From that perspective, the necessity for cultural change should be self-evident. Every aspect of our strategy, planning, budgeting, acquisition, and policymaking should be viewed global, focused on all domains, and employ affordable kinetic and nonkinetic capabilities to address the complex and simultaneous character of future war. Adopting a truly global perspective makes our problems more solvable and affordable. Global plans that start with the homeland and its deterrence requirements should lead to more realistic requirements overall.

Policy, Budgeting, and Acquisitions

Adequate homeland defense requirements cannot be set without a supporting policy in place that outlines exactly what must be defended and to what extent. NORAD and USNORTHCOM must be prepared to protect continuity of government, our nuclear infrastructure, power projection capabilities, and key defense nodes. In addition, these two commands must be prepared to protect key commercial, economic, and utility infrastructure, on both sides of the border, in addition to population centers. Through strong coordination with Office of the Secretary of Defense (OSD) and the Joint Staff, DOD has identified a definitive list of critical assets that will allow for the generation of informed requirements procurement priorities. Moreover, all aspects of policy, including both regulatory and statutory, should be reexamined to ensure that those charged with homeland defense have access to the full range of capabilities in all domains and are not inadvertently constrained by archaic policies written in a different era without consideration that our homeland is being held at risk.

Our acquisition processes are also written for a different era and built to protect from litigation rather than to spur innovation. These processes have reduced litigation risk by adding time-consuming review processes, which in turn have increased risk to national security. It has been this way since after the end of the Cold War. We live in a time where Moore's law, the concept that computing power doubles every 2 years though the cost of computers is halved, is a reality in every commercial and consumer industry. Unfortunately, this truth has not extended to defense technology or operations; we are not fully recognizing and capitalizing on how much technology is amplifying development. This has to change—our innovation requires the same sense of urgency that the Nation had during the Cold War.

To meet today's challenges, we have a range of tools in the science and technology arenas and through organizations such as the Defense Innovation Unit, the OSD Strategic Capabilities Office, and Canada's Innovation for Defence Excellence and Security program. Development of capabilities and systems using the full range of available tools could rapidly bring improved homeland defense to life, make significant headway toward improving homeland defense, and help close a widening gap between strategic and conventional deterrent capabilities.

Mind the Gap

The Nation's strategic nuclear deterrent remains the foundation of its defense. Deterrence by punishment, however, which depends on the adversary's fear of reprisal through nuclear retaliation to defend the United States, is not likely sufficient to address the wide array of threats we face today. For too long, the United States has implicitly relied on and assumed that the strategic nuclear deterrent is adequate to prevent our competitors from attacking our homeland.

In short, we have a deficient complementary conventional homeland defense deterrent capability to defend against or respond to smaller scale conventional attacks on the homeland. This growing gap between our nuclear strategic deterrent and our conventional deterrent capability is specific to our ability to defend the homeland and generate effects right here in North America. Unfortunately, this gap could be exploited by our competitors, kinetically or nonkinetically, with the belief that they might achieve their objectives and remain below the nuclear threshold. In this environment, the threat of a conventional attack on the homeland leaves military and national leaders with a grim choice: either preemptively attack, risking escalation up to or beyond the nuclear threshold, or absorb an attack and be prepared to respond by deploying the force or responding with nuclear weapons. None of these presents a good option. Lack of a credible conventional deterrent also raises the risk that tactical miscalculations could quickly escalate and lead to the possibility of nuclear conflict. While other deterrence options exist to bridge the gap, such as power projection through our long-range non-uclear global strike capability, they too are escalatory in nature.

This capability gap limits our options, constrains our actions, and is potentially more costly in terms of both lives and resources. The gap needs to be closed through the development of flexible and responsive kinetic and nonkinetic conventional deterrents, including information operations that selectively unveil Special Access Program capabilities, and through diplomatic and partnership efforts. Through unambiguous communication of our ability to counter threats below the nuclear threshold, we can achieve deterrence by denial.

Conventional deterrence by denial is additive to deterrence by punishment. Through both, we will complicate a potential adversary's decision calculus, degrade confidence in their planning, and sew doubt in their mind that they can successfully achieve their objectives. The critical capabilities we are developing to deter by denial and close the strategic-conventional deterrence gap are all-domain awareness, information dominance, and decision superiority.

Left of Defeat

We have consistently fixated on kinetic kill capabilities to meet all threats. Leadership, including myself, grew up and achieved success as tacticians and operators first. Kinetic capabilities are what we know and what we are comfortable with. But a reliance on platforms, delivery systems, and weapons alone leads to a responsive, rather than proactive strategy. Senior leaders need to be provided more options than kinetic capabilities. This can be accomplished by drawing attention to the left—left of defeat, and even left of launch, to focus priority efforts on identifying adversary delivery platforms and preconditions for action. We could maintain custody of delivery platforms and weapons from launch to impact, greatly expanding our range of options and time to respond. To accomplish this, we are pursuing a layered-defense approach that emphasizes the use of open data architecture and machine-enhanced processing to move decision space to the left.

The Framework

All-domain awareness is the first element of the framework required to meet today's challenges, especially as NORAD pursues modernization efforts to create a layered network of sensors along the approaches to North America. For air and missile threats, this effort includes enabling early indications and warnings through detection, tracking, identifi-

Marines with Combat Logistics Regiment 25, 2nd Marine Logistics Group, tow Ahkio sled containing cold weather gear, at U.S. Army Northern Warfare Training Center, Alaska, February 20, 2018 (U.S. Marine Corps/Sean M. Evans)

cation, characterization, warning, and attribution. With all-domain awareness and data-sharing, including the use of artificial intelligence (AI) and machine learning, information dominance, the second element of the framework, can be established (that is, the ability to operate inside an adversary observe-orient-decide-act loop). Once information dominance is achieved, decision makers can take action through flexible response options to deny or defeat the threat. These two tools together give us deterrence, and through that, decision superiority, the third element of the framework, from the tactical to the strategic levels of warfare. Creating deterrence, so that we do not have to fight, should be the ultimate goal.

All-Domain Awareness. Our priority within this framework is all-domain awareness sensors and systems that provide persistent and complete battlespace awareness, from subsurface to space and cyberspace. This essential capability increases warning time for national leadership against multiple threats, expanding available response options. Fused data can also be transmitted across the globe to benefit every combatant commander and create global information dominance.

Advancements in all-domain awareness will inform much of the next 2-year budgeting cycle. If we cannot see the threat, we cannot defend against it. Systems such as improved over-the-horizon radars, polar communications through Proliferated Low-Earth Orbit communications, Joint All-Domain Command and Control (JADC2), fixed sea-bed surveillance system, undersea cable-laying ships, polar radars, and counter–small unmanned aerial systems (UAS) detection all appear on NORAD and USNORTHCOM's Integrated Priority List. Investment in these exceedingly capable technologies will ultimately allow the earliest detection of sea-launched cruise missiles and small UAS and hypersonic glide vehicles. It will also give us a significant advantage in the remote regions of the Arctic, which is quickly becoming a key region of global competition.

Information Dominance. The future fight will be won or lost based on our ability to achieve information dominance by connecting data from all-domain awareness sensors to flexible and responsive decision superiority options. Effective information dominance systems must ingest, aggregate, process, display, and disseminate data quickly and reliably by leveraging the potential of AI and machine learning.

Information dominance begins with data. In many cases, the data is global and exists today. However, it needs to be pried from existing stovepipes, flattened, and brought into a DOD cloud-based computing environment in order to enable decision superiority. Decision superiority—the ability able to make faster and better decisions than our potential adversaries—will enable us to deter, deny, and, if necessary, defeat attacks. A flattened data architecture is a prerequisite for this capability and requires cultural change. We need a committed effort to enforce data standards across all echelons and every procurement program and initiative, as well as an increased commitment to data-sharing with allies and partners. The commitment of the Joint Staff's Joint All-Domain Command and Control Cross-Functional Team to lead a new process to set data standards and improve JADC2 interoperability among all sensors and Services is an encouraging step in the right direction.

NORAD and USNORTHCOM are platform agnostic. The particular system chosen is not as important as its ability to be employed globally, across all domains, across all classification levels, and be accessible from the tactical to strategic levels. Affordability and rapid deployment are also key considerations. In redesigning how data is managed, information dominance initiatives, such as the JADC2 concept, will come to fruition and allow the joint force to win in competition or conflict in future information-centric warfare.

Decision Superiority. All-domain awareness and information dominance put decision superiority in the hands of decisionmakers. As a joint force, however, we must not confuse decision superiority with development of traditional kinetic defeat mechanisms. At its heart, decision superiority is about giving senior leaders options. Decision superiority expands the aperture beyond kinetic kill into nonkinetic solutions.

As an example, imagine a future scenario enabled by information dominance and decision superiority tools. In this setting, all-domain awareness sensors detect potentially aggressive activity from a peer competitor, and when processed, machine-enabled insights indicate that the peer competitor is readying bombers for a pending deployment that will heighten regional or global tensions. The analysis, enabled by fusing multiple intelligence and sensor information streams, is performed in a matter of minutes by an AI-enabled system, conducting millions of calculations based on hundreds of images, much more efficiently than human analysts can accomplish. This frees up human operators to conduct higher order processing. The data on the bomber deployment is then used by the system to send an alert to decisionmakers, with a recommendation for courses of action to preposition long-range global strike capabilities or posture friendly air assets to intercept the competitors' aircraft outside of normal ground-based radar detection distances and prior to potential weapons release range. Or perhaps instead of deploying forces, the decisionmaker leverages the information space to message the competitor through action in another combatant commander's area of responsibility or passes the information to the State Department to achieve a diplomatic or political resolution. In any course of action, the competitor's objectives are either dissuaded or diminished based on proactive measures made possible with the expanded decision space.

Such a scenario is not far in the future. Information dominance tools will help us to better understand our competitors' potential courses of action based off of historically informed patterns of behavior and posture a response option at the decisive point ahead of need.

Decision superiority options are needed because our theory of victory cannot only be about achieving kinetic kills; that is a losing strategy, both militarily and financially. It will lead us down the legacy path of focusing on platforms instead of capabilities. Defeat mechanisms are enormously expensive, and when the shooting starts, in a sense, we have *already failed.* Shifting focus left of launch will vector our efforts on identifying earlier indications and warnings—looking at delivery platforms and preconditions for departure while also maintaining custody of air threats and missiles from launch to impact.

Ultimately, we need to get inside our potential adversaries' OODA loops. We need to know when aircrews are stepping to their aircraft, when ships and submarines are planning to sail, and when missile operators and systems are preparing to launch. If we know this information, then through responsive decision superiority options enabled through information dominance tools, it permits the ability to overtly posture the sufficient number of forces before the adversary takes action. This supports a global system to prevent conflict and better defend North America.

Rapid Innovation

NORAD and USNORTHCOM are already moving concepts into prototypes and into operations, bringing an information dominant homeland defense architecture one step closer to reality. Project Convergence, JADC2, and small investments are already showing tremendous improvements in information dominance. One example of a model for the future is the Pathfinder program, which USNORTHCOM and industry partners have been working on for the past year and a half, with contracting assistance from the Defense Innovation Unit.

Pathfinder is now in use at our air defense sectors as a battle management tool. It ingests air domain sensor data from multiple sources, including commercial and military radars; leverages software automation; and uses machine learning models to produce a fused common operating picture and decision superiority tool. Pathfinder did not start by picking a specific solution or platform, and it was not approached as a military problem. Instead, it was approached as a *data* problem for industry partners to solve in order to improve air domain awareness.

With Pathfinder, our Air Battle managers are no longer required to manually correlate and compare track data from multiple sources and systems. Instead, the systems that feed Pathfinder provide a fused track and highlights anomalous behavior. With fused data, both operators and decisionmakers are afforded increased time and decision space.

The next step needed in developing additional tools such as Pathfinder is to aggressively pursue every commercial and military data source, in addition to incorporating data from our allies and partners. Through common data standards and combined networks, we will increase information dominance and achieve true all-domain

Autonomous system Origin prepares for practice run on August 20, 2020, during Project Convergence capstone event at Yuma Proving Ground, Arizona (U.S. Army/Carlos Cuebas Fantauzzi)

awareness. On a larger scale, NORAD and USNORTHCOM are continuing a partnership with the Services and other combatant commands to achieve information dominance. Last year, we partnered with U.S. Space Command and the Air Force in the Air Battle Management System (ABMS) Onramp 2, which was one of the largest joint force demonstrations in the past decade and highlighted the impact of new, innovative, and affordable capabilities against live threats to the homeland. Efforts such as these are serving to flesh out the JADC2 concept for the joint force.

Many attendees left the demonstration talking about and focused on tactical defeat actions, such as a howitzer shooting down a drone simulating a cruise missile. While that was spectacular, it was a secondary benefit and not the main achievement from Onramp 2. The ABMS network established during the demonstration used AI and machine learning capabilities to enable information dominance. These nascent prototype capabilities are what was truly groundbreaking and serve as a model for increasing decision space from the strategic to the tactical level.

The same data environment was used for further experimentation in NORAD and USNORTHCOM's first Global Information Dominance Exercise in December 2020. NORAD and USNORTHCOM—in coordination with U.S. Southern Command, U.S. Indo-Pacific Command, U.S. Transportation Command, U.S. Strategic Command, and the Under Secretary of Defense for Intelligence and Security—convened a digital table-top exercise to prototype cross–combatant command AI-enabled early warning alerts of peer-level threat movements. The scenario was based on historic signal intelligence, electronic intelligence, and satellite imagery. These alerts generated possible enemy course of actions and recommended proactive blue force response options.

While both onramps were successful as demonstrations, they were not enough. The military must continue to provide even more expansive opportunities to highlight the importance of these capabilities to DOD and congressional leadership.

In this new era of rapid Global Power competition, where our competitors are aggressively pursuing advantages in the military, information, economic, and geopolitical ranges, North America is threatened from every vector and all domains. We must accelerate efforts to transform our culture and factor homeland defense into every acquisition, budget, force design, and management decision, so we can maintain advantages, outpace adversaries, and sustain strength at home. Through all-domain awareness, information dominance, and decision superiority, we will deter in competition, deescalate in crisis, and defeat in conflict. JFQ