NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

SUPPLEMENTAL TO DEFENSE ANALYSIS CAPSTONE REPORT

(8 OF 12: APPENDIX H)

USSF CAPABILITY GAP IN THE ARCTIC

by

William B. Martin, Michael K. Tovo,
and Devin L. Kirkwood

December 2022

Thesis Advisor:	Kalev I. Sepp
Second Reader:	Michael Locklear (USASOC)

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

STATEMENT OF

GENERAL GLEN D. VANHERCK, UNITED STATES AIR FORCE

COMMANDER

UNITED STATES NORTHERN COMMAND

AND

NORTH AMERICAN AEROSPACE DEFENSE COMMAND

BEFORE THE SENATE ARMED SERVICES COMMITTEE

24 MARCH 2022

Chairman Reed, Ranking Member Inhofe, and distinguished members of the Committee: thank you for the opportunity to testify today. I am proud to lead the men and women of United States Northern Command (USNORTHCOM) and North American Aerospace Defense Command (NORAD) as we defend the United States and Canada in an increasingly complicated and dynamic strategic environment. Our commands continue to face multiple simultaneous challenges from capable, highly advanced competitors who have openly declared their intent to hold our homelands at risk in an effort to advance their own strategic interests.

Today, strategic competitors, rogue nations, and non-state actors possess the capability to strike institutions and critical infrastructure in the United States and Canada. These threats, along with the realities of modern global competition, drive USNORTHCOM and NORAD to think globally and seek innovative capabilities that increase senior leader decision space and help to expand the range of available options for deterring in competition, de-escalating in crisis, and—if necessary—defeating in conflict.

As the U.S. combatant command responsible for homeland defense, for providing defense support of civil authorities, and security cooperation with allies and partners in our area of responsibility, USNORTHCOM is facing the most dynamic and strategically complex set of challenges in the history of the command. Together with NORAD, the distinct, complementary U.S.-Canada bi-national command responsible for aerospace warning, aerospace control, and maritime warning for the United States and Canada, our commands are taking decisive institutional and operational measures to defend our homelands.

DEFENDING THE HOMELANDS

In my testimony before the Committee last year, I described a rapidly evolving geostrategic environment in which our competitors were continuing to take increasingly

aggressive steps to gain the upper hand in the military, intelligence, economic, and diplomatic arenas. For decades, the United States has been accustomed to choosing when and where the nation will employ the military lever of influence and project power around the globe from a homeland that was assumed to be secure. Our competitors have studied this operating model for the last 30 years and have developed strategies and capabilities intended to offset our military advantage and disrupt our force flows.

Quite bluntly, my ability to conduct the missions assigned to USNORTHCOM and NORAD has eroded and continues to erode. Our country is under attack every day in the information space and cyber domain. Competitors are spreading disinformation, actively sowing division and fanning the flames of internal discord with the intent to undermine the foundation of our nation, our democracy, and democracies around the world. These competitors are also constantly seeking to exploit security vulnerabilities and policy gaps, especially in the cyber domain. They are preparing for potential crisis or conflict with the intent to limit decision space for our senior leaders by holding national critical infrastructure at risk, disrupting and delaying our ability to project power from the homeland, and undermining our will to intervene in a regional crisis.

The threat to North America is complex. Over the last year, our competitors have accelerated their fielding of kinetic and non-kinetic capabilities specifically designed to threaten our homeland. Of equal or greater concern is their relentless, coordinated effort to weaken the institutions and alliances at the core of our strength and influence while expanding their own influence internationally. Today, our competitors hold our homeland at risk in multiple domains and are working constantly to exploit perceived vulnerabilities.

Russia and China continue to aggressively pursue and field advanced offensive cyber and space capabilities, cruise missiles, hypersonic weapons, and delivery platforms designed to evade detection and strike targets in our homeland from multiple vectors of attack and in all domains. USNORTHCOM and NORAD's ability to defend against modern threats requires improved all-domain awareness, updated capabilities, and policies and strategies that reflect the current strategic environment and the advanced capabilities of our competitors. Meanwhile, I require access to ready and trained forces to operate throughout the USNORTHCOM area of responsibility, including the Arctic, to respond in crisis and quickly execute homeland defense campaign plans.

My mission to provide timely and accurate threat warning and attack assessment requires increased domain awareness and breaking down information stovepipes that restrict the flow of needed information to decision makers in the United States and Canada. The ability to detect a threat, whether from a cyber-actor or a cruise missile, is a prerequisite to defeating the threat. Timely and accurate detection, tracking, and assessment of potential threats provides critical decision space and time to national leaders, while an inability to do so limits available response options.

Lack of domain awareness contributes to increased risk of miscalculation, unnecessary escalation, and potential for strategic deterrence failure. Maintaining our strategic advantage begins with improving domain awareness globally, including in the approaches to North America. Incorporating artificial intelligence and machine learning into existing capabilities will allow users to pull needed information from existing data sets and share that data with leaders at all levels to expand their decision space and options necessary to achieve desirable outcomes.

To ensure our ability to compete in the current strategic environment, DoD plans, force structure, and logistics must evolve beyond 9/11-era threats and outdated assumptions regarding competitor capabilities, strategies, and ambitions. In order to deter modern competitors, we must make clear that we have the capability to fight in and from the homeland. Further, policy determinations are needed regarding what key infrastructure is to be defended, and from what threats, in order to develop realistic assessments and plans for the defense of critical infrastructure that fully account for advancing competitor capabilities and strategies.

In order to defend the homeland in this complex strategic environment, USNORTHCOM and NORAD have shifted our efforts to left-of-conflict strategies, emphasizing integrated deterrence in competition, and dramatically improving our ability to provide leaders with needed decision space on a day-to-day basis. To be successful in competition, DoD must develop and implement globally integrated plans, strategies, operations, and exercises that incorporate all levers of influence, to include the essential contributions of our international allies and partners.

COMPETITORS AND THREATS

Russia

Russia is the primary military threat to the homeland, and their focus on targeting the homeland has provided the model other competitors are beginning to follow. First, Russia has invested significant resources to modernize all three legs of its nuclear triad in an effort to ensure its ability to deliver unacceptable damage on our homeland during a conflict. In December 2019, Russia fielded the world's first intercontinental ballistic missiles (ICBMs) equipped with a hypersonic glide vehicle (HGV) payload. These weapons are designed to glide at extremely high speeds and maneuver at low altitudes in order to complicate our ability to detect and track. In the next few years, Russia seeks to field a new heavy-lift ICBM that President Putin claims will

be able to deliver nuclear warheads to North America from both northern and southern trajectories. Weapons such as these are designed to circumvent the ground-based radars utilized by USNORTHCOM and NORAD to detect and characterize an inbound threat, and challenge my ability to provide threat warning and attack assessment. The impact is the loss of critical decision space for national-level decision makers regarding continuity of government and the preservation of retaliatory capabilities, resulting in an increase in the potential for strategic deterrence failure.

Over the last 15 years, Russia has also executed a systematic program to develop offensive capabilities below the nuclear threshold that Russian leaders believe will constrain U.S. options in an escalating crisis. Their capabilities include very capable cyber capabilities like those demonstrated by Russia-based actors during last year's ransomware attack on the Colonial Pipeline. Russia has also invested in counter-space capabilities like the direct-ascent anti-satellite weapon that Russia recklessly tested in November 2021.

To augment these non-lethal capabilities, Russia has fielded a new family of advanced air-, sea-, and ground-based cruise missiles to threaten critical civilian and military infrastructure. The AS-23a air-launched cruise missile, for instance, features an extended range that enables Russian bombers flying well outside NORAD radar coverage—and in some cases from inside Russian airspace—to threaten targets throughout North America. This capability challenges my ability to detect an attack and mount an effective defense. In the maritime domain, Russia has fielded the first two of their nine planned Severodvinsk-class guided missile submarines, which are designed to deploy undetected within cruise missile range of our coastlines to threaten critical infrastructure during an escalating crisis. This challenge will be compounded in the next few years as the Russian Navy adds the Tsirkon hypersonic cruise

missile to the Severodvinsk's arsenal. All of the Russian cruise missile capabilities present a significant domain awareness challenge. Additionally, these advanced cruise missiles and their supporting platforms will limit national leadership decision space and my ability to provide threat warning and attack assessment, which directly influences my ability to support continuity of government operations and provide support to USSTRATCOM missions. Again, the potential consequence is an increased risk of strategic deterrence failure.

China

China is our pacing threat and a long-term geostrategic challenge. China is increasingly exerting its economic and military clout around the globe as its leaders pursue a national goal of supplanting the rules-based international order with an approach that is more aligned with China's national interests. Like Russia, China has begun to develop new capabilities to hold our homeland at risk in multiple domains in an attempt to complicate our decision making and to disrupt, delay, and degrade force flow in crisis and destroy our will in conflict.

China has maintained the ability to strike our homeland with strategic nuclear weapons since the early 1980s, but today its nuclear capabilities are growing rapidly in quantity and sophistication. China's Fractional Orbital Bombardment System test in July 2021 delivered a hypersonic glide vehicle (HGV) and demonstrated the weapon's ability to survive reentry and perform high-speed and maneuvering glide after orbiting around the globe—a feat Russia never attempted before fielding their own HGV-equipped ICBMs two years ago. When fielded, China's ICBM-class HGV will be able to evade current ground and space-based early warning capabilities due to its low-altitude approach and ability to maneuver midcourse, which compounds the detection and warning challenges I already face from Russia's Avangard HGV and advanced cruise missiles.

In the coming years China will augment its homeland-threatening cyber capabilities with a growing long-range conventional strike capability of its own. In October 2019, China unveiled its first bomber capable of air-to-air refueling, the H-6N, which will be able to threaten targets in Alaska with air-launched ballistic or cruise missiles. Later this decade, China seeks to field its Type 095 guided missile submarine, which will feature improved quieting technologies and a probable land-attack cruise missile capability. While China's intent for employing its long-range conventional strike capabilities is not fully known, these weapons will offer Beijing the option of deploying strike platforms within range of our critical infrastructure during a conflict, adding a new layer of complication to our leaders' crisis decision-making.

North Korea and Iran

North Korea's successful flight testing of an ICBM capable of reaching the continental United States and detonation of a thermonuclear weapon underscores its leaders' determination to develop capabilities to threaten our homeland and constrain our options in crisis and conflict. In October 2020, North Korea unveiled a new ICBM that is probably even more capable than the weapons it last tested in 2017. Moreover, North Korea's launch last October of a submarine-based ballistic missile suggests Kim Jong Un may soon resume flight testing his most capable weapon systems, including a new ICBM design.

Iran maintains asymmetric capabilities to threaten our homeland in the cyber domain. In 2022, Iranian officials have threatened to carry out terror operations inside the United States and elsewhere around the world, in addition to its persistent support of threats by terrorist organizations like Lebanese Hezbollah. While Iran has announced a self-imposed range limit of 2,000 kilometers on its fielded ballistic missile force, its persistent advancement of ballistic missile technologies probably could increase its missile range outside of the region.

Violent Extremist Organizations

While the strategic capabilities of our peer competitors are the most pressing concern for USNORTHCOM and NORAD, violent extremist organizations such as ISIS and al-Qa'ida remain committed to attacking the United States and our allies. The Taliban's takeover in Afghanistan will likely provide new opportunities for groups like al-Qa'ida to plot against the West, while homegrown violent extremists (HVEs) challenge our law enforcement partners by using simple attack methods that continue to present the most likely international terrorist threat to the homeland. Violent extremist groups continue to hone their tactics in response to a shifting operational environment and have maintained their focus on attacking civil aviation and U.S. military personnel and installations.

Transnational Criminal Organizations

Transnational Criminal Organizations (TCOs) continue to inflict enormous damage and create instability through corruption, violence, and illicit trafficking. International criminal syndicates have flooded the United States with illegal drugs that contributed to the deaths of over 100,000 U.S. citizens in the 12-month period from April 2020 to April 2021, while harming people and weakening institutions throughout the Western Hemisphere. As TCOs battle over territory and brazenly undermine the rule of law, they create obvious opportunities for exploitation by strategic competitors seeking to broaden their global coercive strategies and increase influence and presence in the Western Hemisphere.

Mitigating the harm done by TCOs is a national security imperative for the United States and our international partners that requires an overarching whole-of-government policy and plan for interagency action that takes into consideration the vast resources and widespread influence wielded by the TCOs and their international criminal confederates. USNORTHCOM's ability to

counter malign influence in our region is complicated by the destabilizing influence of TCOs in our area of responsibility, and national policy and DoD planning must take that reality into account.

INTEGRATED DETERRENCE

Strategic deterrence remains the foundation of homeland defense, and I believe it is absolutely necessary to maintain a reliable and effective nuclear triad. However, reliance on deterrence by cost imposition is currently over-weighted and significantly increases the risk of miscalculation by limiting our national leaders' options following an attack. Given our competitors' advanced conventional capabilities, it is vitally important to move toward a model of integrated deterrence that employs all elements of national influence, leverages alliances and partnerships, and provides leaders with a wide range of timely deterrence options.

Integrated deterrence fuses traditional deterrence by cost imposition—in which an adversary is deterred by fear of costs that outweigh the benefit of an attack—with deterrence by denial, which causes a potential adversary to doubt the likelihood of a successful attack. Imposing costs on an aggressor that outweigh the potential benefits of an attack, demonstrating resiliency, and displaying a range of kinetic and non-kinetic response capabilities are all elements of deterrence by denial. This approach dramatically expands the military, diplomatic, and economic options available to national leaders in competition, crisis, and conflict and helps to avoid miscalculation and unnecessary escalation.

Integrated deterrence also involves competing in the information space under a strategic framework, while working with allies and partners to counter competitors' malign influence in the USNORTHCOM area of responsibility and beyond. Building the capacity to compete in the

information environment reduces the risk of instability and strategic miscalculation that can stem from disinformation and other influence operations.

Demonstrations of resiliency, hardening, and the ability to recover from damage to communities and infrastructure also generate a deterrent effect. USNORTHCOM's defense support of civil authorities (DSCA) mission in the aftermath of wildfires, hurricanes, floods, and other contingencies in communities across the United States routinely showcases the ability of USNORTHCOM and the interagency community to respond quickly and effectively to natural and manmade disasters.

USNORTHCOM's track record of supporting coordinated responses and rapid recovery is the direct result of ongoing interagency planning, coordination, and exercises that ensures our readiness to support our partners at a moment's notice. To be clear, DSCA is a homeland defense mission, and USNORTHCOM's visible support to civil authorities remains a critical focus for the command, especially as environmental change contributes to more frequent and intense fires and damaging storms.

Finally, we must continue to foster the partnerships and alliances that provide the United States and our international partners with what is perhaps our most distinct asymmetric advantage. NORAD is an obvious example of the enormous benefit to shared security and regional stability generated by international cooperation. In addition, it must be noted that our relationships with NATO, the FIVE EYES community, and our regional defense and security cooperation partners in Canada, Mexico, and The Bahamas have a profound deterrent effect for the common benefit of all. USNORTHCOM and NORAD continue to foster these valuable alliances and partnerships.

HOMELAND DEFENSE DESIGN

Homeland defense starts well outside the USNORTHCOM area of responsibility and necessarily involves our fellow combatant commands as well as our international allies and partners. Deterring and defending against advanced competitors that have the capability to hold the homeland at persistent risk requires an approach that emphasizes increased decision space and leverages all elements of national power over cost-prohibitive and narrowly focused kinetic defenses. DoD's ability to deter and defend against advanced global threats requires a shift from regional approaches to a global perspective that accounts for the realities of the modern strategic environment.

I believe it is necessary to accept near-term risk in order to compete against advanced, globally focused peers well into the future. Leaders must make difficult choices today in order to avoid impossible dilemmas tomorrow—to include divesting legacy systems and capabilities that consume significant personnel and fiscal resources and are of little to no use in today's strategic environment.

Therefore, a homeland defense enterprise that is capable of deterring and defeating threats is essential to a globally integrated forward fight and supporting broader national strategic objectives. The ability of the United States to deter in competition, de-escalate in crisis, and defeat in conflict is dependent on our collective ability to detect and track potential threats and friendly forces anywhere in the world, while delivering data to decision makers as rapidly as possible. This provides leaders with the time and informed options needed to achieve a favorable outcomes for the United States. That reality is the basis for the central principles of USNORTHCOM and NORAD homeland defense design: **all-domain awareness, information dominance, decision superiority, and global integration**.

Domain Awareness can be achieved through an integrated network of sensors from the seafloor to space, including cyberspace, in order to detect, track, and deter potential threats. I need improved domain awareness to increase warning time and provide leaders at all levels with as many options as possible to deter or defend against an attack. Global all-domain awareness will generate a significant deterrent effect by making it clear that we can see potential aggressors wherever they are, which inherently casts doubt on their ability to achieve their objectives.

I am grateful to the Committee for your support of the over-the-horizon radar (OTHR) that was included on USNORTHCOM's unfunded priority list for Fiscal Year 2022. OTHR is a proven technology that will provide persistent surveillance of the distant northern approaches to the United States and mitigate the limitations of the Cold War-era North Warning System, while contributing to broader domain awareness challenges including space domain awareness. The ability to detect air-breathing and space-borne threats in the approaches to Canada and the United States will be significantly enhanced by fielding OTHR as soon as possible. It is also vital to move quickly toward advanced space-based sensors capable of detecting hypersonic weapons, including hypersonic cruise missiles, and other advanced systems designed to evade detection. Modernizing and expanding the Integrated Undersea Surveillance System (IUSS) is equally important as Russia and China continue to field highly advanced guided missile submarines.

While some new domain awareness platforms will be required, it is possible to make exponential improvements in our nation's ability to detect and track potential threats by improving the ways data is collected, processed, and shared. As I testified last year, the technology already exists to apply artificial intelligence and machine learning to collect and rapidly distribute information gathered from sensors around the globe. Current processes rely on human analysts to comb through enormous volumes of data, and it can take days or weeks to

process, exploit, and distribute critical information—if it is ever processed at all. We will always need expert human analysts in the loop, but I need the ability to tap into that technology to dramatically speed the delivery of information to leaders at all levels who need it.

Success in competition, crisis, and conflict depends on effectively distributing and integrating the data collected from domain awareness capabilities to establish **information dominance** over competitors and adversaries. To unlock the full value and potential of our intelligence and sensor networks, information must be integrated, appropriately classified, and rapidly shared to allow commands, agencies, allies, and partners to collaborate globally in real time and across all domains.

The potential for this capability has already been demonstrated in USNORTHCOM's Global Information Dominance Experiments (GIDE), which provided combatant commanders, intelligence and operations directors, and other participants at multiple sites with a shared, customizable, and near real-time data set. The data gathered by existing global sensors provided leaders, analysts, and operators with the information needed to make assessments and recommended courses of action that were coordinated across multiple commands in a matter of hours. Speeding the flow of information to senior civilian decision makers and commanders enabled significantly more options to achieve desired outcomes.

Decision superiority means increasing decision space and options to provide senior leaders. The ultimate goal of decision superiority is to provide multiple paths to avoid conflict through the application of all available elements of national power, rather than emphasizing options that are only available after a conflict has already begun. To successfully defend the homeland, we must provide leaders with pertinent information and as much time as possible to deter and de-escalate before a situation escalates out of control.

Finally, I believe it is critical for the entire defense enterprise to shift its culture and vision toward global all-domain integration. Too often, DoD posture development, communications, planning, exercises, and operations are stove-piped and isolated in ways that do not reflect the reality that all challenges are global and all-domain in nature. The Department increasingly understands that competitors would likely intend to strike the homeland in an effort to prevent flowing U.S. forces toward a regional crisis or conflict. And, in the event that the United States and our allies become engaged in a regional crisis or conflict, other competitors would likely exploit that opportunity to their own advantage—which could quickly lead to simultaneous crises in multiple theaters.

Global challenges cannot be overcome with a hodgepodge of isolated regional plans. Success in competition, crisis, or conflict is increasingly dependent on moving past outdated parochial approaches in favor of greater focus on competition rather than restricting options and absorbing unnecessary costs by continuing to over-emphasize crisis and conflict. With that in mind, USNORTHCOM, our fellow combatant commands, the Services, and our Canadian partners have demonstrated the immediate impact of improved information sharing and collaboration between commands and allies in all phases of competition, crisis, and conflict.

The current regional approach to plans, strategies, and force design is outdated and more influenced by bureaucratic inertia than the realities of the modern strategic environment. The same is true of stagnant acquisition practices and cumbersome civilian hiring rules that only impede progress and hinder the Department's ability to move at the speed of relevance necessary to compete in today's environment.

RISK MITIGATION

Risk mitigation must be a shared whole-of-government responsibility focused on broad nodes, enterprises, and capabilities rather than attempting to establish a priority-ranked list of specific sites or facilities to be protected. Mitigating the risk associated with an attack on the United States requires policy determinations about what must be defended from kinetic and non-kinetic attack. Those policy decisions, in turn, allow USNORTHCOM, NORAD, and our mission partners to determine the best ways to protect priority assets and resources.

Importantly, risk mitigation is the responsibility of the DoD, as well as a number of other interagency partners at the federal, state, and local levels. Risk mitigation requires a dedicated policy framework and deliberate interagency planning and coordination. Notably, the deterrent effect of resiliency and effective consequence management requires far fewer resources and less expense than direct defense systems.

Ballistic missile defense (BMD): Defending the United States against intercontinental ballistic missile (ICBM) threats from rogue nations remains a critical priority for USNORTHCOM and an important component of integrated deterrence. While current BMD capability and capacity is sufficient to defeat a limited ballistic missile attack from a rogue nation, North Korea's ongoing development of increasingly complex and capable strategic weapons requires the Next Generation Interceptor to be fielded on time or early, and for the Long Range Discriminating Radar in Alaska to achieve full operational capacity on schedule.

The ballistic missile defense system is not capable of intercepting hypersonic glide vehicles; I cannot defend, nor am I tasked to defend, against a hypersonic glide vehicle attack. It is imperative that the Department of Defense develop and field an integrated space-based domain awareness network capable of detecting and tracking ICBMs, hypersonic weapons, and cruise

missiles as quickly as possible. I require the ability to detect, track, and assess potential missile threats of all types to immediately determine whether an attack is underway and provide national leaders with as much time and as many options as possible.

Cruise Missile Defense: Russia has the capability today to hold targets in the United States and Canada at risk with long-range air- and submarine-launched conventional cruise missiles. These highly precise and stealthy systems highlight the need for policy determinations regarding what must be defended along with continued demonstrations of resiliency and hardening. It is also necessary to quickly improve domain awareness by fielding sensors such as OTHR and the integrated undersea surveillance system (IUSS)—and by integrating and sharing the collected data with global stakeholders. To successfully deter aggression and defend the homeland, we must be able to detect and track the submarines, aircraft, and surface ships that carry weapons systems capable of striking the homeland before they depart from their home stations. We also need to improve our capability to defeat those launch platforms before they are within range of their targets.

It is vital that we accept risk today in order to compete against highly advanced and determined peers in the near future. As an example, the military Services must be allowed to retire aging platforms, especially those that cannot survive in combat against highly advanced and lethal capabilities already fielded and proliferated by our peer competitors. The Department must re-invest the savings from those divestments to resilient domain awareness and other capabilities necessary to increase the decision space that will provide national leaders with options to deter, de-escalate, and defeat threats. Those difficult choices are critical to integrated deterrence today and avoiding the unthinkable tomorrow.

THE ARCTIC

The Arctic demonstrates how regional challenges increasingly take on global implications that require a global framework. The Unified Command Plan designates the Commander of USNORTHCOM as the DoD's Advocate for Arctic Capabilities in recognition of the fact that the region encompasses a vast geographic area overlapping the areas of responsibility of three separate geographic combatant commands and includes eight sovereign nations with inherent interest in the region. It is critical that USNORTHCOM, our fellow geographic combatant commands, the U.S. interagency, and our fellow Arctic nations continue our shared efforts to ensure the Arctic remains peaceful, stable, prosperous, and cooperative. This is especially true in light of the increasing potential for resource competition and opportunities for commercial enterprise, both of which must be balanced with the inherent rights of Arctic states to control their territorial waters and resources within their Exclusive Economic Zones.

Diminished Arctic ice has led to increased access to sea lanes, longer shipping seasons, and expanded access to subsurface minerals and proteins, although environmental changes are also increasing operational hazards and introducing new uncertainties. Those changes, in turn, now require clear communication and coordination among Arctic allies, partners, and competitors. A continued rules-based international order in the Arctic has served the international community well for decades, and forums like the Arctic Council are critical to emphasizing the value of the Arctic as a cooperative region where countries consistently work together to solve shared challenges.

Rising competition near the United States and Canada is of significant concern for USNORTHCOM and NORAD. The Arctic strategies published by DoD and each of the military

Services demonstrate the shared understanding of the need to adapt policy, capabilities, and resourcing to meet the challenges and requirements associated with operating in the Arctic. However, the Services and the Department must accelerate implementation of those strategies or risk falling further behind rapidly advancing competitor capabilities, which jeopardizes USNORTHCOM and NORAD's ability to execute the commands' missions in the high north.

Likewise, Canada remains our essential partner in the NORAD mission and in ensuring NORAD's capability and capacity to deter aggression and defend the United States and Canada from airborne and maritime threats. That contribution includes investment in modernizing sensors, infrastructure, and platforms that ensure NORAD's ability to successfully conduct aerospace warning, aerospace control, and maritime warning. Those capabilities are vital to homeland defense and to our nations' capability to project forces forward in support of operations overseas, including meeting NATO commitments.

I am excited by the opportunities for building partnerships in the Arctic and the continued shared effort to maintain the stability and security of the entire region. The upcoming Arctic Security Forces Roundtable, to be held in Alaska in May 2022, will provide the United States with a rare opportunity to host an international forum focused specifically on Arctic security and military cooperation. USNORTHCOM and NORAD have important roles at the Arctic Security Forces Roundtable, and I am looking forward to joining Arctic military counterparts to make this a productive and forward-thinking event.

Likewise, the newly established DoD regional center, the Ted Stevens Center for Arctic Security Studies, in Anchorage will provide an important venue for academic, diplomatic, and military Arctic experts to address key challenges in the region, in alignment with DoD strategic guidance. None of those challenges, from mitigating the operational impacts of climate change

to avoiding miscalculation resulting from undue militarization of the Arctic, can be overcome unilaterally. USNORTHCOM will continue to leverage the strength of our regional alliances and partnerships to enhance regional security cooperation and support a secure and stable Arctic.

DEFENSE SUPPORT OF CIVIL AUTHORITIES (DSCA)

USNORTHCOM's defense support of other federal agencies during the COVID-19 pandemic, hurricanes, wildfires, and Operation ALLIES WELCOME has tested the command in unexpected ways over the past year. While our DSCA mission can be time- and resource-intensive, USNORTHCOM support to our interagency partners continues to strengthen relationships, validate plans, and demonstrate the ability of the U.S. interagency enterprise to respond quickly and effectively to contingencies. In addition to supporting American citizens in need, these missions provide a visible deterrent effect by demonstrating flexible response options and effectively executing plans to mitigate and recover from the effects of disaster and other emergencies.

In 2021 and 2022, USNORTHCOM continued DoD's COVID-19 support by deploying military medical providers to civilian medical facilities around the country. Building on existing pandemic response plans and quickly adapting to lessons learned during the pandemic, USNORTHCOM's support to the Federal Emergency Management Agency and the Department of Health and Human Services provided much-needed relief to hospitals overwhelmed by COVID-19 caseloads.

USNORTHCOM is also proud to work alongside the Department of Homeland Security and the Department of State throughout the Operation ALLIES WELCOME mission to evacuate, house, and resettle tens of thousands of Afghan partners and their families following the collapse of the Afghan government. With the support of the military departments, USNORTHCOM has

been responsible for providing safety and security, shelter, food, and other essential services for Afghans who contributed to the U.S. mission in Afghanistan as they await resettlement in the United States.

SECURITY COOPERATION

Global alliances and partnerships provide the United States with a critical asymmetric advantage over our competitors. USNORTHCOM's military-to-military partnerships with Canada, Mexico, and The Bahamas remain critically important, and those ties continue to pay significant dividends as we work toward improving regional security, strengthening military ties with regional partners, and expanding interoperability. These efforts contribute to improved shared domain awareness and domain control, while strengthening the institutions that support our common strategic objectives. By working together toward these objectives, USNORTHCOM is supporting our partners' important contributions to regional security while emphasizing our shared prioritization of the rule of law, human rights, and denying our competitors the opportunity to expand their presence and malign influence.

The Mexican Secretariat of National Defense (SEDENA) and Secretariat of the Navy (SEMAR), are steadfast security partners and remain a bulwark against encroaching competitor presence and influence in Central and South America. USNORTHCOM was proud to host the annual U.S.-Mexico Bilateral Military Cooperation Roundtable in August 2021, during which key military leaders from USNORTHCOM, SEDENA, and SEMAR refined our shared efforts toward improved domain awareness, domain control, and institutional strengthening. In September 2021, I was also honored to personally attend the Mexico Aerospace Fair—commonly known as FAMEX—to demonstrate USNORTHCOM's commitment to the security relationship with our Mexican military partners and to join the Secretaries of SEMAR and

SEDENA in reaffirming Mexico's vital contributions to the security of our region and our shared commitment to countering common threats.

Our partnership with The Bahamas remains critical. USNORTHCOM and The Bahamas' Bilateral Security Cooperation Framework provides a distinct and important venue for developing and implementing mutual objectives that contribute to regional security. Due to The Bahamas' geographic location along the U.S. southern approaches, domain awareness and domain control are in the vital national interests of both the United States and The Bahamas. In October 2021, I met with the new Bahamian government and my Royal Bahamas Defence Force counterpart in Nassau for the activation of a maritime surveillance radar donated by DoD that has already significantly improved our collective ability to detect and monitor traffic in the approaches to The Bahamas and the United States. China has expanded economic investment and visible diplomatic presence in The Bahamas and has highlighted the lack of a confirmed U.S. ambassador in an ongoing information campaign to boost Chinese influence while weakening that of the United States.

CONCLUSION

The global strategic environment will remain complex and extraordinarily dynamic for the foreseeable future. Our competitors already possess the capability to strike the homeland with kinetic and non-kinetic means, and they will take full advantage of slow responses, technological shortfalls, and policies that do not reflect the realities of the modern era.

USNORTHCOM and NORAD, in concert with our interagency colleagues, will continue our unending mission to defend our homelands and protect our citizens from threats in all domains, institutions, culture, and process. However, our commands' ability to effectively deter threats to the homeland will increasingly rely on improved domain awareness and providing

leaders with the time and options necessary for success. Just as important, it is critical for military leaders and civilian policymakers to acknowledge that all regional challenges have global implications and present potential risk to the U.S. homeland. Our competitors have demonstrated their intent to leverage any opportunity to advance their own interests—often to the detriment of our own.

Defense of the homeland and continental defense remains the absolute priority for both USNORTHCOM and NORAD, and our commands' constant vigilance will be a key element of the integrated deterrence that safeguards our citizens and advances our vital national interests. It is my profound honor to lead all of the proud U.S. and Canadian military and civilian personnel of USNORTHCOM and NORAD as they stand our never-ending watch over our nations. I look forward to working with all of our vital partners as we continue to advance those efforts in the defense of our nations. We Have the Watch.