

THE WATCH



GREAT POWER COMPETITION

TRUTH DETECTIVES
AGENCY FIGHTS FOREIGN PROPAGANDA

ARCTIC VIEWS
CANADA, U.S. EXPERTS OUTLINE VISIONS

JOINING HANDS
POLAND, U.S. DRAWING CLOSER

CONTENTS

THE WATCH // GREAT POWER COMPETITION



Today, we are experiencing one of the most dynamic geostrategic environments I have ever seen in my 33 years of service. Whether the threat comes from Russia, China, Iran, North Korea, violent extremist organizations, transnational criminal organizations or cyberspace, the challenges posed by potential adversaries will persist. I believe that we must continue to evolve our culture and mindset and lead our defense establishments to ensure that every operational plan, decision and budgeting choice we make as an institution starts and ends with homeland defense.”

— U.S. AIR FORCE GEN. GLEN D. VANHERCK

COMMANDER OF U.S. NORTHERN COMMAND
AND THE NORTH AMERICAN AEROSPACE DEFENSE COMMAND

v3

Features

From *The Watch* Staff **04**

DEPARTMENTS

Impressions **05**

Innovation **12**

Health Watch **20**

World View **28**

Flashback **42**

Rapid Response **52**



06

Arm in Arm

Defense pact between Poland, U.S. designed to deter Russian aggression.

14

Defending the Homeland

NORAD and USNORTHCOM commander outlines priorities, highlights capabilities.

22

Dominating the Next-Gen Battlespace

U.S. military's innovative Advanced Battle Management System takes leap forward.

30

Fighting for the Truth

U.S. Global Engagement Center combats disinformation and propaganda.

36

Arctic Views

Canadian, U.S. experts provide perspectives on this contested environment.

46

Building Resilience

U.S., allies face tests posed by technology and great power rivals.

54

Rethinking Supply Chains

Pandemic exposes weaknesses in China-centric processes.

60

Agile and On Guard

NORAD hones air defenses, readiness with Arctic exercise.

64

Arctic Deterrence

Denmark may use stealth F-35s over Greenland.

ABOUT THE COVER

This illustration by *The Watch* depicts an era of great power competition involving the People's Republic of China, Russia and the United States.

DEAR READERS,

An emerging era of great power competition presents complex challenges for homeland defenders in areas as wide-ranging as disinformation campaigns to supply chain vulnerabilities. In this edition of *The Watch*, we explore how these challenges are strengthening alliances, igniting technological development and invigorating efforts to counter harmful propaganda.

As NATO allies collaborate to deter an aggressive Russia, the United States is establishing a permanent military presence in Poland. The defense pact signed in August 2020 is a guarantee, Polish President Andrzej Duda said, that in case of a threat “our Soldiers are going to stand arm in arm.”

Such alliances are vital because competitors, including the People’s Republic of China (PRC) and Russia, continue to demonstrate the capability and intent to harm the national interests of the U.S., making the roles of U.S. Northern Command (USNORTHCOM) and the North American Aerospace Defense Command (NORAD) more important than ever. In one article, U.S. Air Force Gen. Glen D. VanHerck, commander of USNORTHCOM and NORAD, outlines his vision for outpacing adversaries through technological innovation and information dominance.

That shared vision brought together more than 130 teams from government, industry and every branch of the U.S. Armed Forces in dozens of locations in August and September 2020 to further field test the Advanced Battle Management System, which relies on artificial intelligence, machine learning and virtual reality to repel attacks against the U.S. homeland.

Homeland defenders must dominate adversaries in all domains because threats do not all materialize in the form of planes, bombs or missiles. Fierce battles are being waged in the information arena, and the U.S. Global Engagement Center is on the front lines. The center combats propaganda and disinformation from Russia, Iran, the PRC and terrorist groups to stop adversaries from weakening democratic institutions or promoting civil unrest.

To make sure adversaries cannot threaten North America from the icy approaches of the Arctic, Canadian and U.S. experts are devising strategies to create a layered defensive ecosystem that includes military assets and information operations. And, finally, challenges posed by the global coronavirus pandemic in 2020 combined with threats from great power adversaries have demonstrated the need for defense strategies to focus on resilience. From vulnerable cyber infrastructure to China-centric supply chains, homeland defense experts are strengthening systems and duplicating supply networks to champion resilience as a strategy.

As *The Watch* continues to spark dialogue about homeland defense issues, we invite you to contact us at n-nc.peterson.n-ncj3.mbx.the-watch@mail.mil with your perspectives.

Regards,
THE WATCH STAFF



THE WATCH

Homeland Defense

Volume 3 2021

USNORTHCOM LEADERSHIP

GLEN D. VANHERCK
General, USAF
Commander

MICHAEL P. HOLLAND
Rear Admiral, USN
Chief of Staff

MARSHALL SMITH
Program Manager

CONTACT US

THE WATCH

The Watch
Program Manager
HQ USNORTHCOM
250 Vandenberg St., Suite B016
Peterson AFB, CO 80914-38170
email:

n-nc.peterson.n-ncj3.mbx.the-watch@mail.mil

The Watch is a professional military magazine published by the commander of U.S. Northern Command to provide an international forum for military personnel involved in homeland defense. The opinions expressed in this magazine do not necessarily represent the policies or points of view of the command or any other agency of the U.S. government. All articles are written by *The Watch* staff unless otherwise noted. The secretary of defense has determined that the publication of this magazine is necessary for conducting public business as required by the Department of Defense.

ISSN 2577-0098 (print)



A paratrooper from the U.S. Army's Spartan Brigade climbs a wall during mountaineering training at Joint Base Elmendorf-Richardson, Alaska. Paratroopers from the scout platoon of the 1st Battalion, 501st Infantry Regiment (Airborne), 4th Brigade Combat Team (Airborne), 25th Infantry Division, conducted the training in October 2020. The Spartan Brigade is the only airborne infantry brigade combat team in the Arctic.

MAJ. JASON WELCH/U.S. ARMY



ARM **IN** ARM

Defense pact between Poland, U.S. designed to deter Russian aggression

THE WATCH STAFF

The United States is establishing a significant military presence in Poland as the NATO allies collaborate to defend their homelands and keep a watchful eye on an increasingly assertive Russia. The defense pact between Poland and the U.S. signed in August 2020 represents a pledge by the allies to fight Russian aggression in areas ranging from cyberspace to combating disinformation.

U.S. Secretary of Defense Lloyd J. Austin III spoke by phone in mid-February 2021 with Polish Minister of Defence Mariusz Błaszczak to “reinforce the importance of the longstanding U.S.-Poland strategic alliance,” Pentagon Press Secretary John Kirby said in a statement. The defense leaders discussed a range of issues, including Poland’s commitment to defense modernization, the U.S. rotational force presence in Poland and regional security. They also emphasized the significance of the recent Enhanced Defense Cooperation Agreement.

During the signing ceremony in 2020, Polish President Andrzej Duda characterized the pact as an important milestone. “This is going to be an extended guarantee: a guarantee that in case of a threat, our Soldiers are going to stand arm in arm,” Duda said, according to The Associated Press (AP). “It will also serve to increase the security of other countries in our part of Europe.”

The agreement allows for the enhancement and modernization of existing capabilities and facilities by allowing U.S. forces access to Polish military installations. It also provides a formula for cost sharing. “The opportunities are unlimited. The resources will be available,” then-U.S. Secretary of State Mike Pompeo said at a news conference alongside Polish Foreign Minister Jacek Czaputowicz, AP

“This is going to be an extended guarantee: a guarantee that in case of a threat, our Soldiers are going to stand arm in arm. It will also serve to increase the security of other countries in our part of Europe.”

— Polish President Andrzej Duda

reported. “Troop levels matter ... but the world has moved on, too,” Pompeo said, referring to threats posed in space and cyberspace and through disinformation campaigns. He said the defense pact would allow joint work on those threats.

The defense agreement places a sharp focus on Russia, which annexed Crimea from neighboring Ukraine in 2014. It “enhances our deterrence



U.S. Navy Lt. Cmdr. Tim Zakriski notates the position of helicopters while working in the aircraft control tower of the amphibious assault ship USS Wasp. The Wasp was conducting anti-submarine warfare training during the U.S. Navy's Exercise Black Widow in September 2020.

PETTY OFFICER 2ND CLASS
ERIC SHORTER/U.S. NAVY

Polish Soldiers in August 2020 mark the centennial of the Battle of Warsaw, a Polish military victory that stopped the Russian Bolshevik march.

THE ASSOCIATED PRESS



Then-U.S. Secretary of State Mike Pompeo, left, and Polish Minister of Defence Mariusz Blaszczak greet each other with an elbow bump in August 2020 after signing a defense cooperation agreement at the presidential palace in Warsaw. AFP/GETTY IMAGES

potential because we are closer to the potential source of conflict,” Czaputowicz said. The deal, which took months to negotiate, will strengthen NATO’s deterrence efforts and help free countries in Europe and around the world. “The agreement will enhance our military cooperation and increase the United States’ military presence in Poland to further strengthen NATO deterrence, bolster European security, and help ensure democracy,

freedom, and sovereignty,” then-President Donald Trump said in a statement.

GEOGRAPHIC SIGNIFICANCE

Poland has long been a major focus of NATO efforts to deter Russian aggression in Europe. A key reason is that Poland is on NATO’s eastern perimeter and provides land access to the Baltic states. Although Ukraine is not a NATO ally, the Russian occupation of the Crimea signaled to many military observers that NATO allies, “particularly those in Eastern Europe, could once again be threatened by Moscow,” according to a July 2020 analysis published by Eurasia Review. “In response, the United States and its NATO allies have undertaken a number of initiatives to emphasize NATO’s collective defense agreements, thereby assuring allies of their own security while simultaneously deterring Russian aggression.”

The U.S. focus on Poland prompted speculation about how Russia might react. “The situation is complicated by Kaliningrad, a 5,800-square-mile Russian exclave wedged between Poland and Lithuania,” the Eurasia Review analysis states. “Kaliningrad is a key strategic territory for Russia, allowing the country to project military power into NATO’s northern flank. The territory has a

DETERRENCE AT SEA:

USN 2nd Fleet protects vital shipping lanes

U.S. NAVY 2ND FLEET

At the forefront of the deterrence effort against Russian military operations is the U.S. Navy's 2nd Fleet (C2F), which was revived in 2018 to combat the increasing challenge of Russian submarine threats while also addressing employment of Navy forces in the Arctic.

As the Arctic opens up, North Atlantic shipping lanes will become more important as the U.S. and its European allies forge closer ties to protect each other's homelands. "Within an increasingly complex global security environment, our allies and competitors alike are well aware that many of the world's most active shipping lanes lie within the North Atlantic," said Vice Adm. Andrew Lewis, commander of C2F.

The fleet's structure is inherently flexible to help address 21st century challenges. The Maritime Operations Center (MOC), the heart of the organization that directs the ships, submarines, aircraft and other units assigned to the fleet, is designed to be modular and rapidly deployable, adapting to meet any assigned mission. The MOC deployed in the Baltic to lead the multinational BALTOPS 2019 exercise; to Keflavik, Iceland, to command and control a surface action group as it traversed the Atlantic Ocean; and to Camp Lejeune, North Carolina, as part of a naval integration exercise with the U.S. Marine Corps.

This flexibility is necessary because the C2F can be called to operate in the Atlantic or the Arctic, portions of which are in the areas of responsibility (AOR) of U.S. Northern Command (USNORTHCOM) and U.S. European Command (USEUCOM). C2F's ability to modify its command and control arrangement lets it integrate across the Atlantic with U.S. Navy 6th Fleet counterparts — a visible representation of the U.S. commitment to security in the Atlantic, the Arctic and the European theater.

This arrangement recognizes the growing challenge of Russian submarine operations. Submarines from Russia's Northern Fleet must maneuver through the Greenland-Iceland-United Kingdom gap before entering the Atlantic. Critically important during the Cold War, these waters are divided between the commanders of USNORTHCOM and USEUCOM. This seam between geographical combatant commands can be stitched together by a fleet specifically designed to operate seamlessly.

Protecting North America isn't just a job for the U.S. Navy. Lewis also is commander of Joint Force Command Norfolk (JFCNF), a NATO command established to support readiness and defend lines of communication and resupply routes in the North Atlantic. JFCNF brings the perspectives of U.S. allies such as Canada, Denmark, France and Norway to C2F operations.

This helps the staff develop plans to address challenges ranging from anti-submarine warfare to integrating defensive cyberspace into routine operations.

"JFC Norfolk's mission is fundamentally joint and multinational," Lewis said at the command's initial operational capability ceremony, "requiring close coordination across all warfighting domains, with close cooperation among various national and allied commands working in the region."

"A ready-to-fight mentality remains our highest priority. I expect that ships, aircraft and marine units operating in the C2F AOR are fully trained, qualified and proficient in order to expertly handle the full range of combat operations."

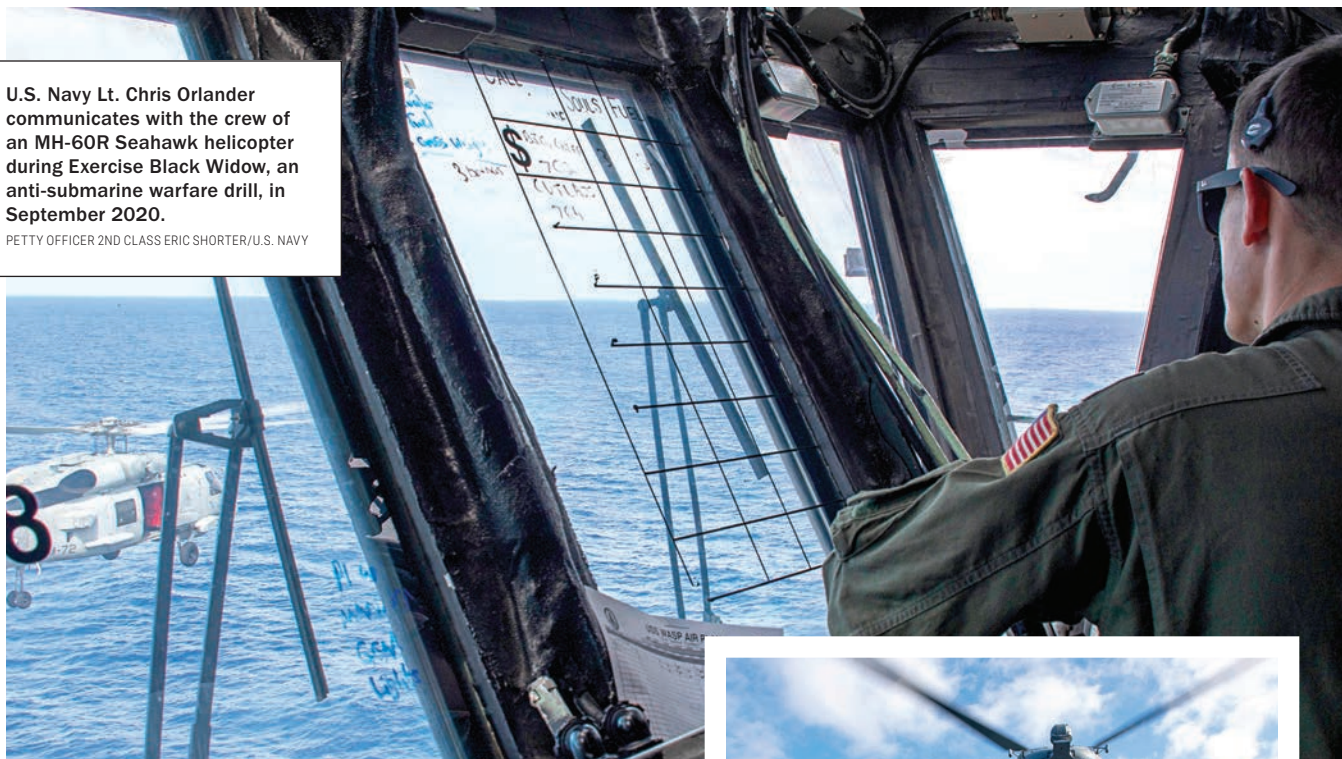
— Vice Adm. Andrew Lewis,
commander of C2F

Deterring adversaries requires these new approaches because the Atlantic Ocean is considered contested space. All U.S. Navy ships and submarines that operate in the Atlantic must be ready to fight, regardless of their phase of training. Fleet guidance recently issued by Lewis made this perfectly clear. "A ready-to-fight mentality remains our highest priority. I expect that ships, aircraft and marine units operating in the C2F AOR are fully trained, qualified and proficient in order to expertly handle the full range of combat operations," he said.

C2F in 2019 directed the USS Mahan, an Arleigh Burke-class, guided-missile destroyer, to monitor the Russian Navy's intelligence ship Viktor Leonov. The Mahan was in the middle of its overseas certification process when it was called into action. Its reports about the Leonov's unsafe actions, such as operating in fog with no running lights and not responding to the hails of nearby merchant ships, served as notification for the U.S. Coast Guard to warn nearby vessels through a maritime safety information bulletin. The Mahan's readiness to conduct maritime surveillance on short notice is testament to the new realities of great power competition.

U.S. Navy Lt. Chris Orlander communicates with the crew of an MH-60R Seahawk helicopter during Exercise Black Widow, an anti-submarine warfare drill, in September 2020.

PETTY OFFICER 2ND CLASS ERIC SHORTER/U.S. NAVY



heavy Russian military presence, including the Baltic Fleet and two airbases. Russia has deployed Iskander short-range nuclear-capable missiles in Kaliningrad.”

“We very much like the support, the agreement between the United States and Poland. We understand this is not only for Poland, but it’s also about the Baltic countries.”

— Lithuanian Defense Minister Raimundas Karoblis

SUPPORT FROM BALTICS

It’s that proximity to Poland and the heavy Russian presence on its doorstep that has Baltic countries praising the defense support from the U.S. “We very much like the support, the agreement between the United States and Poland,” Lithuanian Defense Minister Raimundas Karoblis told the Washington



A U.S. Navy aircrewman performs a search-and-rescue hoist drill during Canadian Operation Nanook in the Atlantic Ocean. The operation involved U.S., Canadian, Danish and French allies and was designed to increase their Arctic capabilities. SEAMAN SAWYER CONNALLY/U.S. NAVY

Examiner, a U.S.-based news website and weekly magazine. “We understand this is not only for Poland, but it’s also about the Baltic countries. The Baltic countries and Poland are treated as one region from a defense point.”

Polish General Staff Air Force Lt. Col. Tomas Pietrus told the website that the positioning of U.S. troops in Poland deters Russia in the east. “We are on the eastern front of NATO,” he said on the sidelines of air defense exercises at Siauliai Air Base in Lithuania. “So, we need to be able to operate, to defend ourselves firstly, then the coalition.”

The defense cooperation agreement is an important signal to Russia, the Lithuanian defense minister said. “The signaling is very important, both for the deterrence and the defense factor,” he said. ▣



U.S. AIR FORCE RESEARCH LABORATORY

SKYBORG PROGRAM HAS ROBOTIC WINGMAN ASSIST HUMAN PILOTS

THE WATCH STAFF

The U.S. Air Force Research Laboratory is developing robotic vehicles that will operate with manned aircraft in contested airspace.

The Skyborg program combines autonomous vehicle technology, seamless connectivity and open architecture to suppress enemy defenses and execute other missions, *Forbes* magazine reported in August 2020. The program's name apparently derives from the *Star Trek* television series and refers to a threat so menacing that "resistance is futile."

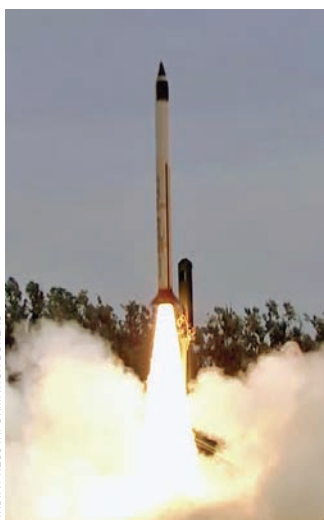
The Skyborg program represents a radical approach to air warfare. The Air Force describes the program as a low-cost, teamed aircraft that can "thwart adversaries with quick, decisive actions in contested environments."

Pilots would receive key information about their surroundings when the robotic aircraft, pictured, detect potential air and ground threats, determine threat proximity and analyze danger. "Embedded within the

teamed aircraft, complex algorithms and cutting-edge sensors enable the autonomy to make decisions based on established rules of engagement set by manned teammates," the Air Force Research Laboratory stated on its website.

Air Force policy stipulates that people are always responsible for lethal decision-making, so Skyborg will not replace human pilots. Instead, it will provide them with data to support rapid decisions.

INDIA LATEST NATION TO TEST HYPERSONIC TECHNOLOGY



INDIA PRESS INFORMATION BUREAU

THE WATCH STAFF

India reported in September 2020 that it had successfully tested hypersonic technology, becoming only the fourth country in the world to do so.

It was already among the small group of nations that possess nuclear weapons, and only the People's Republic of China, Russia and the United States had previously tested hypersonic weapons.

Hypersonic weapons are considered unstoppable because they can travel at least five times the speed of sound and are extremely maneuverable, making them hard to strike down with missiles.

A statement from India's Defence Research and Development Organisation (DRDO) noted that the test demonstrated the platform's capabilities.

"The @DRDO_India has today successfully flight

tested the Hypersonic Technology Demonstrator Vehicle using the indigenously developed scramjet propulsion system," Indian Defence Minister Rajnath Singh posted on Twitter. "With this success, all critical technologies are now established to progress to the next phase."

Indian Prime Minister Narendra Modi responded that the test vehicle traveled at six times the speed of sound. "Very few countries have such capability today," Modi tweeted.

Hypersonic missiles can travel with computerized precision while descending back into Earth's atmosphere. Although they can be armed with nuclear warheads, the speed and force of a hypersonic missile allow it to inflict damage by sheer kinetic impact without the need for explosives.



PHILIPS RESEARCH NORTH AMERICA

WEARABLE TECH OFFERS PROMISE OF EARLY COVID-19 DETECTION

THE WATCH STAFF

The U.S. military is testing wearable technology that could provide early detection of COVID-19. A watch and a ring can detect biometric indicators such as slight changes in skin temperature, the U.S. Department of Defense said in a news release. Military leaders hope the technology, powered by artificial intelligence and machine learning, can ensure military readiness.

The Defense Threat Reduction Agency (DTRA) and Defense Innovation Unit are testing the Rapid Analysis of Threat Exposure, or RATE, technology, which consists of noninvasive wearable devices that provide warning of infection up to 48 hours before a person becomes symptomatic, said Ed Argenta, DTRA science and technology manager.

Like a check-engine warning for drivers, the system is designed to alert Soldiers when they need to pursue diagnostic testing. RATE uses off-the-shelf wearables to measure key biomarkers and processes the data in the cloud so users can see their hourly RATE score on a secure website.

Researchers discovered that exposure to infectious agents causes subtle changes in physiology before symptoms surface. Identifying these changes early is critical to containing the spread of the disease by asymptomatic and pre-symptomatic individuals, Argenta said. It could also accelerate preventive measures such as quarantine.

U.S., U.K. TEAM UP TO CONQUER DATA HURDLES

THE WATCH STAFF

Sensors allow military forces to see, hear and understand their battlefield environment by producing data related to enemy activities, capabilities and location. A key challenge is how to rapidly process the massive amounts of data into usable information.

The United States and United Kingdom recently announced a jointly funded project to automatically process data obtained from sensors and optimize that information for mission success. The project is led by the U.S. Army Combat Capabilities Development Command Army Research Laboratory, CCDC-Atlantic, and the U.K. Defence Science and Technology Laboratory. It represents a new concept for such research projects between the nations, the U.S. Army reported on its website.

The project will include various aspects of processing data and information from networks of heterogeneous sensors, particularly autonomous sensors, operating without a centralized computing node. The research will address three questions: how to manage task and resource allocation for autonomous sensors; how to maintain computational effectiveness of the network of sensors in an environment with many simultaneous targets; and how to characterize and quantify uncertainties in sensor-derived estimates. (Pictured: A U.S. Army Soldier operates a Black Hornet unmanned aerial system. The display screen, which is slightly larger than a smartphone and attached to his vest, provides situational awareness.) The research team received a U.S. \$1.2 million grant over three years. The science and technology workforce from both governments were involved with the call for proposals, which encouraged “development of mathematical analysis and algorithms, rather than hardware.”

“Emerging technologies such as cheap, lightweight uncrewed aerial vehicles provoke a need for research into information processing of data derived from multiple autonomous sensors,” said Alasdair Hunter, the lead researcher from the U.K. “In the military context, sensors have to work in a potentially contested environment, so networks of sensors are required to be resilient against attack and failure of individual sensors and communication links. This project addresses the challenges arising from the design of resilient networks by developing novel, fundamental information processing algorithms.”



U.S. ARMY

DEFENDING THE HOMELAND

AND OUTPACING THE ENEMY

NORAD and USNORTHCOM commander outlines priorities, highlights capabilities

THE WATCH STAFF



The United States can expect to see adversaries continue to demonstrate the capability and intent to threaten national interests in this era of renewed power competition, but U.S. Air Force Gen. Glen D. VanHerck said that North American Aerospace Defense Command (NORAD) and U.S. Northern Command (USNORTHCOM) stand ready to meet those challenges and outpace opponents.

“USNORTHCOM’s essential role in defending the nation and supporting federal and international partners will be more vital than ever as the command continues to meet its sacred obligations,” VanHerck said in prepared remarks for a U.S. Senate Armed Services Committee hearing to confirm his appointment. He pledged to ensure an adaptive and responsive command while mitigating the coronavirus pandemic’s effects on military readiness and public health.

“This historic confluence of challenges highlights the necessity for a dedicated and focused combatant command, a ready and responsive force and continued modernization of our homeland defense architecture.”

NORAD is a binational command of the U.S. and Canada charged with the missions of aerospace warning, maritime warning and aerospace control for North America. USNORTHCOM conducts homeland defense, civil support and security cooperation to protect the U.S. and its interests. The two commands have complementary missions and are co-located at Peterson Air Force Base in Colorado Springs, Colorado.

VanHerck assumed command of NORAD and USNORTHCOM in August 2020. He previously served

as director of the Joint Staff at the Pentagon, where he assisted the chairman of the Joint Chiefs of Staff in advising the U.S. president and defense secretary, coordinated and directed activities of the Joint Staff in support of the chairman and served as the staff inspector general. VanHerck, who has served as an instructor pilot and flight examiner as well as a U.S. Air Force weapons school instructor, succeeded U.S. Air Force Gen. Terrence J. O’Shaughnessy, who retired from active duty after 34 year of military service.

VanHerck “has a keen understanding of the nature of today’s threats and the importance of greater investments to advance our capabilities and make tangible strides toward decision superiority, which puts us ahead of our adversaries at every single turn,” then-U.S. Secretary of Defense Mark Esper said during a change of command ceremony. “He’s committed to ensuring NORTHCOM and NORAD lead the way in preparing our military across every domain.”

The path to victory in such a dynamic battlespace includes information dominance, VanHerck said.

“I’m a firm believer that future competition, crisis and conflict will be won or lost based on our ability to achieve information dominance,” the commander wrote in his initial guidance published in a NORAD and USNORTHCOM newsletter. “This will drive requirements for critical data to support decisions from the strategic to the tactical level. To get there, we need domain awareness across every environment, from subsurface to on-orbit and cyberspace. We must continue to develop and provide all-domain command and control.”







Chairman of the Joint Chiefs of Staff Army Gen. Mark Milley, right, administers the oath of office to U.S. Air Force Gen. Glen D. VanHerck, commander of the North American Aerospace Defense Command and U.S. Northern Command, in August 2020.

JHOMIL BANSIL/U.S. DEFENSE DEPARTMENT

VanHerck “has a keen understanding of the nature of today’s threats and the importance of greater investments to advance our capabilities and make tangible strides toward decision superiority, which puts us ahead of our adversaries at every single turn.”

~ Mark Esper, then U.S. Defense Secretary

VanHerck outlined near-term priorities and his mission focus in the newsletter. They include:

- **Homeland defense:** “As the National Defense Strategy and Sensitive Site Exploitation state, defense of our North American homelands is our No. 1 priority,” VanHerck said. “It is a no-fail mission.”
- **All-domain awareness:** “We must continue working through this to lead cultural changes within the U.S. Department of Defense and Canadian Armed Forces and ensure support for domain awareness improvements necessary to better defend the homelands,” he said.
- **Defense support of civil authorities:** “We must be ready daily to support our interagency partners, when requested, especially in this COVID environment,” VanHerck said.
- **Ballistic missile defense capabilities:** “In collaboration with [the U.S.] Missile Defense Agency (MDA), we must ensure there are no gaps in capability and achieve a true layered defense for our nations,” he said.

VanHerck outlined additional focus areas. “Foster and maintain a healthy and fun work environment, foster and maintain relationships, grow leaders and execute today’s fight efficiently and effectively,” he said, adding that he highlights these priorities each time he’s tapped as a commander.

“Today, we are experiencing one of the most dynamic geostrategic environments I have ever seen in my 33 years of service,” VanHerck wrote in the command’s newsletter. “Whether the threat comes from Russia, China, Iran, North Korea, violent extremist organizations,



A North American Aerospace Defense Command F-22 Raptor intercepts a Russian bomber entering the Alaskan Air Defense Identification Zone in June 2020. REUTERS

transnational criminal organizations or cyberspace, the challenges posed by potential adversaries will persist. I believe that we must continue to evolve our culture and mindset and lead our defense establishments to ensure that every operational plan, decision and budgeting choice we make as an institution starts and ends with homeland defense.”

BALLISTIC MISSILE DEFENSE

USNORTHCOM’s mission includes defending the U.S. against the threat of ballistic missile attack. To do so, U.S. ballistic missile defense systems must remain operationally effective and keep pace with evolving threats posed by rogue states, VanHerck said. USNORTHCOM works closely with the MDA to ensure that system sustainment and testing provide the command the capability to execute its ballistic missile defense mission, VanHerck said. Test flights help inform successful deployment and capabilities and build warfighters’ confidence in U.S. systems.

Working with the MDA, USNORTHCOM evaluates current and emerging technology that enhances missile defense capabilities against threats such as North Korean ballistic missiles and missile attacks from the People’s Republic of China (PRC) and Russia. “The threat of large-scale missile attacks from Russia and China can be effectively addressed through strategic deterrence,”



Members of the Canadian Air Defence Sector at 22 Wing North Bay, Ontario, take part in a North American Aerospace Defense Command air defense exercise over the Beaufort Sea and Thule Air Base, Greenland, in August 2020.

CPL. ROBERT OUELLETTE/ROYAL CANADIAN AIR FORCE

VanHerck said in his congressional remarks.

The U.S. achieves deterrence by investing in hypersonic weapons and science and technology research programs, including developing a space-based sensor layer to complement current and planned terrestrial-based sensor architecture, he said. Such a layer places hundreds of satellites in low-Earth orbit to track hypersonic missiles and ballistic threats. Such sensors, characterized as terrestrial combat, can also be used to collect tactical intelligence.



“As adversaries’ missile threat capabilities evolve, I believe we must have the ability to continuously track and discriminate every threat from the time of launch through intercept,” VanHerck told Congress. “A space-based sensor layer could provide near-global coverage, tracking and discrimination for a wide spectrum of missile threats.”

NORAD works with mission partners to enhance air defense systems and domain awareness sensor coverage of the northernmost region of North America. VanHerck called the development of such capabilities a priority. “We must be able to defend North America against the cruise missile threat,” he said.

OUTPACING THE ADVERSARY

The U.S. and Canada face diverse threats and challenges to their air defenses across domains. NORAD and

Members of the Royal Canadian Air Force’s Snowbirds aerial demonstration team, left, greet guests at the North American Aerospace Defense Command’s 60th anniversary ceremony at Peterson Air Force Base in Colorado. STAFF SGT. EMILY KENNEY/U.S. AIR FORCE

Marines disembark a U.S. Army CH-47 Chinook after a raid on a long-range radar site at Fort Greely, Alaska, during U.S. Northern Command exercise Arctic Edge 2020.

LANCE CPL. JOSE GONZALEZ/U.S. MARINE CORPS



USNORTHCOM “work around the clock” to monitor these approaches and stand ready to respond at a moment’s notice should adversaries challenge the command’s defense, VanHerck said. Near-peer competitors such as the PRC and Russia, for example, seek to exploit perceived vulnerabilities to erode the U.S.’s strategic advantage, he said. The PRC and Russia have changed the global strategic dynamic by fielding long-range weapons that can reach North America from well beyond NORAD’s radar coverage area. They are also increasingly aggressive in seeking to expand their global presence and influence, VanHerck said.

“Our adversaries continue to advance capabilities with increasing ranges, speed and maneuverability. I believe North American Aerospace Defense Command’s air and missile warning systems must outpace our adversaries’ advancing capabilities by providing detection and warning at ranges that allow an appropriate response,” VanHerck told Congress.

NORAD’s modernization efforts will ensure its systems outperform competitor capabilities. VanHerck said he will continue to advocate for improvements to ensure the command maintains a strategic and tactical advantage.

PROTECTING ARCTIC INTERESTS

USNORTHCOM’s area of responsibility has included the Bering Strait and the North Pole since the 2011 Unified Command Plan realigned combatant command boundaries. That means USNORTHCOM protects U.S. sovereignty and interests in the Arctic region, where the PRC and Russia are jockeying for influence. VanHerck said USNORTHCOM’s Arctic requirements will be assessed to identify gaps or shortfalls that would impede the command’s mission. “I believe it is imperative the command have the ability to operate, communicate and maintain domain awareness in the Arctic,” he said, adding that achieving success there will involve collaborating with U.S. European Command and U.S. Indo-Pacific Command.

The commander also highlighted the value of established relationships and forums that facilitate open communication among Arctic stakeholders regarding operational requirements, such as the USNORTHCOM-led Arctic Capabilities Advocacy Working Group.

VanHerck said that he supports the U.S. formally joining the United Nations Convention on the Law of the Sea, which established a comprehensive framework of rules relating to the world’s oceans and seas. The U.S. is the only Arctic nation that has not signed the 1982 treaty, and VanHerck said that allows revisionist powers such as the PRC and Russia to advance their interests by exploiting the U.S. absence in key diplomatic forums. Joining the treaty, VanHerck said, would ensure that U.S. interests are represented during international negotiations regarding territorial disputes and challenges to maritime customs and practices. ▣



LACK OF TRANSPARENCY

Health organization faces backlash for deference to China

Indo-Pacific Defense FORUM

With the world watching, a global health body deferred to political pressure from the Chinese Communist Party as Chinese officials tried to obscure the genesis of a worldwide coronavirus pandemic. The controversy surrounding the actions of the World Health Organization (WHO) in the pandemic's early stages led the United States to initially withdraw from the agency. As investigations continue into the origins of COVID-19 and the WHO's response, more than 108 million people had been infected and 2.4 million had died worldwide by mid-February 2021.

Taiwan Health Minister Chen Shih-chung, far right, parliament members and activists conduct a news conference in May 2020 about Taiwan's efforts to join the World Health Organization. REUTERS

QUESTIONABLE INFLUENCE: While publicly lavishing praise on the People's Republic of China (PRC) for its transparency in fighting the virus, WHO officials privately complained about Beijing's refusal to hand over data after the disease was first detected in Wuhan, China. WHO officials even lambasted countries for imposing travel bans on Chinese citizens.

"Beijing has never been shy about using every tool in its toolkit to pursue its agenda, and global organizations play an important role in that objective," Daniel Wagner, chief executive officer at Country Risk Solutions, said. Wagner, a widely published author on public affairs issues who has worked in risk management in the Indo-Pacific, summed up the PRC's goals: "Beijing is in the process of creating an alternative world order based on its unique world view, which sees Chinese interest as paramount."

The WHO did not declare COVID-19 a global emergency until January 30, 2020, during a meeting in which WHO Director-General Tedros Adhanom Ghebreyesus of Ethiopia profusely thanked the PRC for its

The WHO did not declare COVID-19 a global emergency until January 30, 2020, during a meeting in which WHO Director-General Tedros Adhanom Ghebreyesus of Ethiopia profusely thanked the PRC for its cooperation.



Tedros Adhanom Ghebreyesus, director-general of the World Health Organization, wears a mask after leaving a ceremony in Geneva in June 2020. Tedros has come under fire for his agency's response to the COVID-19 pandemic. AFP/GETTY IMAGES

cooperation. "We should have actually our respect and gratitude to China for what it's doing," he said, according to The Associated Press (AP). "It has already done incredible things to limit the transmission of the virus to other countries."

Tedros won the election to lead WHO in 2017 over a candidate from the United Kingdom because of fierce lobbying by Beijing and 50 African states. Tedros worked closely with the PRC when he was Ethiopia's health minister during a time when his country was borrowing billions from the PRC. Just months after taking the helm at WHO, he named former Zimbabwe dictator Robert Mugabe, a notorious human rights violator, a goodwill ambassador. Tedros backed down after an international uproar ensued.

"Diplomats said [Mugabe's] appointment was a political payoff from Tedros Adhanom Ghebreyesus – the WHO's first African director-general – to the PRC, a longtime ally of Mugabe, and the 50 or so African states that helped to secure Tedros' election earlier this year," columnist Rebecca Myers wrote in the U.K.'s *The Sunday Times*

newspaper in October 2017.

The WHO's deference to Beijing was not without consequence. The U.S. suspended payments to the health organization for 60 days in April 2020 pending an investigation into what officials called an information cover-up and mismanagement of the crisis. The U.S. eventually decided in early 2021 to rejoin the WHO under newly elected President Joe Biden, pledging to restore funding and work with the global body to advance therapeutics and vaccines worldwide.

POLITICAL PRESSURE: Although Taiwan is viewed as having achieved success in stopping the spread of COVID-19, it remains locked out of WHO membership due to the agency's relationship with the PRC. The extent of the PRC's influence over the WHO went viral in March 2020 when a top WHO official not only avoided a reporter's questions about Taiwan but also hung up on her when she persisted.

By mid-February 2021, Taiwan's population of nearly 24 million had recorded only 937 COVID-19 cases and nine deaths. Taiwan

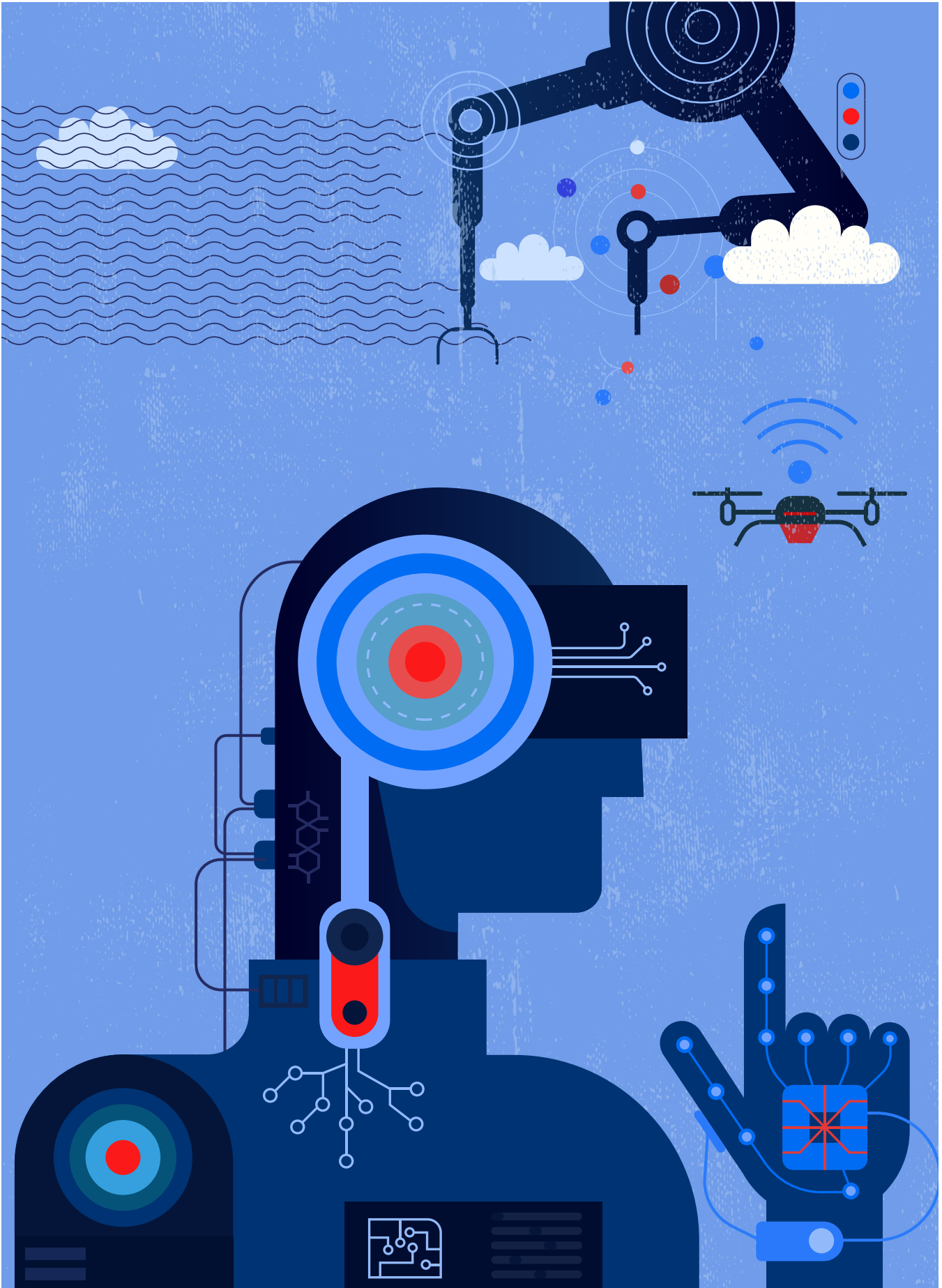
officials argued they should not be left out of the pandemic discussion when they had pertinent information to share. Taiwan health officials emailed WHO on December 31, 2019, asking for more information about "atypical pneumonia cases." Getting no response, Taiwan instituted health screenings that day for all flights from Wuhan and charged ahead with protecting its citizens. On January 26, 2020, Taiwan became the first country to ban inbound flights from Wuhan. Besides quarantining travelers early in the spread of the disease, Taiwan's COVID-19 measures included closely monitoring people in quarantine.

"We hope through the test of this epidemic the WHO can recognize clearly that epidemics do not have national borders. No one place should be left out because any place that is left out could become a loophole. ... Any place's strength shouldn't be neglected so that it can make contributions to the world," Taiwan Health Minister Chen Shih-chung said at a news conference.

Questions concerning the WHO's response to the pandemic run much deeper, however, than its exclusion of Taiwan. An AP investigation revealed that while WHO officials praised the PRC throughout January 2020 for its speedy public health response and for sharing the genetic map of the virus "immediately," officials inside the agency were privately complaining that they were not receiving timely medical data. Chinese officials refused to release the genetic map of the deadly virus for more than a week after multiple government labs had fully decoded it. Records obtained by the AP show that WHO officials were frustrated that the PRC was stonewalling at a time when the outbreak could have been slowed.

"We're currently at the stage where yes, they're giving it to us 15 minutes before it appears on CCTV," WHO's top official in China,

Dr. Gauden Galea, said in one meeting, referring to the state-owned China Central Television.



DOMINATING THE NEXT-GEN BATTLESPACE

U.S. military's
innovative
Advanced Battle
Management
System takes leap
forward

THE WATCH STAFF

A “sci-fi awesome” display of U.S. technical ingenuity and military power and precision has turbocharged development of next-generation warfighting capabilities that promise to redefine homeland defense for the hypersonic age.

More than 130 teams from government, industry and every branch of the U.S. Armed Forces gathered in dozens of locations in August and September 2020 to further field test the Advanced Battle Management System (ABMS), which the U.S. Air Force calls the “backbone of a network-centric approach” to 21st century warfare.

During the weeklong exercise, or onramp, military operators tapped into nascent technology such as artificial intelligence (AI), machine learning and virtual reality to identify and repel simulated attacks against the United States, including its space-based operations. In the “culminating punch,” a U.S. Army M109 Paladin 155 mm howitzer shot down a surrogate cruise missile

AT&T technicians and civilian contractors assemble a “Cell on Wings” drone to provide 5G connectivity to participants in the Advanced Battle Management System onramp at White Sands Missile Range, New Mexico, in August 2020.

STAFF SGT. CHARLYE ALONSO/U.S. AIR FORCE





with a hypervelocity projectile, according to Dr. Will Roper, assistant secretary of the Air Force for acquisition, technology and logistics.

“Tanks shooting down cruise missiles, that’s just awesome,” Roper told reporters. “That’s video game, sci-fi awesome.”

“And hypervelocity gun weapons systems are precisely the very mobile, scalable, high-density defense, with a low cost per kill, that can help us here in the homeland or could help defend a base and a forward-operating location far from home against a similar threat,” he said.

The second ABMS onramp, which followed an initial three-day exercise at Eglin Air Force Base in Florida in December 2019, involved about 1,500 participants at military bases, test ranges and other sites stretching from Maryland to New Mexico and Nevada to the Gulf of Mexico.

In the battlespace of tomorrow, combatants will be saturated with information, Roper said. The onramp tested the ability of personnel and systems to almost instantaneously synthesize and operationalize a tidal wave of data from myriad sources.

“We were able to fuse those into a common operational picture that warfighters understood, that provided information that was actionable at machine speeds that in

As part of the ABMS exercises at Nellis Air Force Base, Nevada, in September 2020, U.S. Air Force Tech. Sgt. John Rodriguez provides security with a Ghost Robotics Vision 60 prototype.

TECH. SGT. CORY D. PAYNE/U.S. AIR FORCE

the past would have taken 20 or 30 minutes to aggregate that we were able to do in a matter of seconds,” he said.

“You’re not supposed to be able to shoot down a cruise missile with a tank,” Roper added. “But, yes, you can if your bullet is smart enough, and the bullet that we used for that system is exceptionally smart.”

For Air Force Gen. Glen D. VanHerck, the exercise highlighted two crucial aspects of the revolutionary system: The ABMS augments but does not replace human decision-making; and in machine learning, the machine itself is learning in real time.

“What we saw as it took a look at the threat over and over, it digested more of what that threat capability looked like and gave us a higher percentage of confidence,” VanHerck, commander of U.S. Northern Command and



A U.S. Air Force Airman from the 62nd Airlift Wing guides an M142 High Mobility Artillery Rocket System from a C-17 Globemaster III during ABMS exercises at Nellis Air Force Base.

TECH. SGT. CORY D. PAYNE/
U.S. AIR FORCE

the North American Aerospace Defense Command, told reporters. “And so, as a combatant commander, that is very appealing to me to get a system like that — that will learn and provide additional capability.”

‘A LEAGUE OF ITS OWN’

The need for speed is accelerating the modernization of battlefield capabilities and missile defense systems, as the pace of development and deployment of hypervelocity weapons quickens.

“In today’s era of great power competition, as new technologies alter the character of warfare, we must stay ahead of our near-peer rivals — namely China and Russia,” then-U.S. Secretary of Defense Mark Esper said in a speech at the U.S. Department of Defense (DOD) Artificial Intelligence Symposium and Exposition in September 2020, days after the ABMS onramp.

In December 2019, Russia announced the deployment of its first hypersonic nuclear-capable missile, which it claims can travel at 27 times the speed of sound, or about 33,000 kilometers per hour, The Associated Press reported.

That came just two months after China’s People’s Liberation Army debuted a hypersonic glide vehicle during a military parade, according to the DOD’s September

2020 report to the U.S. Congress titled “Military and Security Developments Involving the People’s Republic of China 2020.”

In the face of such rapidly developing threats, Esper said, “artificial intelligence is in a league of its own, with the potential to transform nearly every aspect of the battlefield, from the back office to the front lines.”

Development of the ABMS nests within a comprehensive reimagining of U.S. warfighting operations fueled by what Esper called the “tectonic impact” of game changers such as machine learning and AI. In 2018, the Pentagon established the Joint Artificial Intelligence Center as a centerpiece of its road map to adopt and scale AI. Among other projects, the center is exploring how AI-enabled predictive analytics can amplify human-machine collaboration to elevate decision-making.

“Our initial focus is creating decision-support tools for front-line commanders that will be critical in an evolving operational environment where speed, precision and agility are paramount for success,” Dana Deasy, the DOD’s chief information officer, said at the September 2020 symposium.

With historic levels of funding committed in this domain, Esper noted, the U.S. will “outpace our strategic competitors and maintain our military overmatch.”



A dish antenna relays commands for a “Cell on Wings” drone to provide 5G connectivity during ABMS exercises at White Sands Missile Range.

STAFF SGT. CHARLYE ALONSO/U.S. AIR FORCE



“History informs us that those who are first to harness once-in-a-generation technologies often have a decisive advantage on the battlefield for years to come,” he told symposium attendees.

‘THE KEY TO NEXT-GEN WARFARE’

The U.S. Air Force has budgeted U.S. \$3.3 billion over five years for ABMS development, which it identifies as its No. 1 modernization priority.

“To win the contested, high-end fight, we need to accelerate how we field critical technologies today,” Air Force Chief of Staff Gen. Charles Q. Brown Jr. said in a September 2020 statement. “Rapid, iterative experimenting ultimately places relevant capability in warfighters’ hands faster.

“We cannot afford to slow our momentum on ABMS,” Brown added. “Our warfighters and combatant commands must fight at internet speeds to win.”

When fully functional, the system will serve as the cornerstone of the DOD’s Joint All-Domain Command and Control (JADC2) initiative encompassing all military branches and domains — air, land, sea, space and cyberspace.

ABMS teams from the U.S. government, military and defense industry are developing algorithms and software that glean and analyze data gathered by aircraft, satellites, ships and ground-based sensors, among other sources. Real-time data dissemination speeds and streamlines multidomain decision-making, eliminating information silos among disparate command-and-control systems.

During the second ABMS onramp, teams confronted a range of scenarios, including scrambling fighter jets to defend against a simulated cruise missile-capable air threat and intercepting and destroying a target drone masquerading as a cruise missile. Operators used digital technology such as virtual reality and augmented reality, while the use of tablet computers put command-and-control functions in commanders’ hands.

Data pulled from sources including missile-warning radar, acoustic sensors and prototype sensor towers that



U.S. Air Force Lt. Col. James Forrest operates a virtual reality headset during ABMS exercises in September 2020 at Joint Base Andrews, Maryland. SENIOR AIRMAN DANIEL HERNANDEZ/U.S. AIR FORCE

Members of the U.S. Coast Guard from the Maritime Security Response Team East interdict a vessel in support of ABMS exercises in September 2020 in the Gulf of Mexico.

STAFF SGT. HALEY PHILLIPS/U.S. AIR FORCE

combine radar and electro-optical infrared cameras was delivered to the cloud through 4G and 5G communication systems. That enabled “a kill chain that took seconds, not minutes or hours to complete,” Roper said.

“Potential adversaries are investing heavily in these fields, and we must exploit new approaches to sustain the advantage,” U.S. Chief of Space Operations Gen. John “Jay” Raymond said in a news release. “We are exploring how to use JADC2 and ABMS to link sensors to shooters across all battlespaces, at speed and under threat. Maturing these concepts and capabilities is necessary to fight and win in the information age.”

Roper said the exercise cemented military leaders’ growing trust in AI and analytics. “Valuing data as an essential warfighting resource, one no less vital than jet fuel or satellites, is the key to next-gen warfare,” he said.

Future ABMS onramps likely will be scheduled on a four-month cadence and eventually will incorporate U.S. allies and partners, according to the Air Force. Capabilities will be rolled out for operational use as they prove their mettle during testing.

VanHerck said that any skepticism he had about the potential of AI and machine learning was blown away by the potency on display at the second onramp.

“For me, as a warfighter, this is about all-domain operations and all-domain command and control,” he said. “I don’t care where the information comes from or how it gets there, I just need the information to be decision-quality. For domain awareness, it gives me information dominance for decision superiority.” ■

QATAR



U.S. SPACE FORCE DEPLOYS TO ARABIAN PENINSULA

THE ASSOCIATED PRESS

The newly formed U.S. Space Force is deploying troops to a vast new frontier: the Arabian Peninsula. Space Force has a squadron of 20 Airmen stationed at Qatar’s Al Udeid Air Base in its first foreign deployment.

The force represents the sixth branch of the U.S. military and the first new military service since the creation of the Air Force in 1947.

Future wars may be waged in space, but the Arabian Desert already saw what military experts dub the world’s first space war — the 1991 Desert Storm operation to drive Iraqi forces from Kuwait. Today, the U.S. faces new threats in the region from Iran’s missile program and efforts to jam, hack and blind satellites.

“We’re starting to see other nations that are extremely aggressive in preparing to extend conflict into space,” Col. Todd Benson, director of Space Force troops at Al Udeid, said. “We have to be able to compete and defend and protect all of our national interests.”

In a September 2020 swearing-in ceremony at Al Udeid,

pictured, 20 Air Force Airmen entered Space Force, with several more expected to join the unit of space operators who run satellites, track enemy maneuvers and try to avert conflicts in space.

Concerns over the weaponization of outer space are decades old. As space becomes increasingly contested, however, military experts have cited the need for a space corps devoted to defending U.S. interests. Threats from global competitors have grown since the Persian Gulf War in 1991, when the U.S. military first relied on GPS coordinates to tell troops where they were in the desert as they pushed Iraqi dictator Saddam Hussein’s forces out of Kuwait.

Benson did not name the nations his Airmen will monitor, but the decision to deploy Space Force personnel at Al Udeid followed months of escalating tensions between the U.S. and Iran.

Hostilities between the countries came to a head in January 2020 when U.S. forces killed a top Iranian general. Iran responded by launching ballistic missiles at U.S. Soldiers in Iraq.

SWEDEN

DEPLOYMENT BOLSTERS EFFORTS IN BALTIC SEA REGION TO DEFEND SOVEREIGNTY



Sweden stepped up its defense activities in the Baltic Sea region in August 2020 due to what a high-ranking official called “a deteriorating security situation” as Russia and NATO conducted military operations there.

The Swedish Armed Forces said they initiated a “high-readiness action,” pictured, in the southeastern and southern Baltic Sea region due to the “current, extensive military activity.” Sweden is not a NATO member. The military said the goal “is to strengthen maritime surveillance in the Baltic Sea at sea and from the air.”

The Baltic News Service reported that four Russian naval ships were detected near Latvian territorial waters. Two frigates from a NATO maritime force were to visit the Lithuanian port of Klaipeda. “Extensive military operations are underway in the Baltic Sea region, both from Russia and the West, in a way that in some parts has not been experienced since the days of the Cold War,” Vice Adm. Jan Thornqvist, the Swedish military’s chief of joint operations, said.

In a statement, he said it was the military’s assessment “that the risk of a military attack on Sweden is currently low, but the unpredictable security situation in our immediate area places high demands on our accessibility and preparedness.

“We follow, we adapt, and we choose methods in our way of meeting the world around us,” Thornqvist said.

THE ASSOCIATED PRESS



CHINA

LEAKED DATABASE REVEALS CHINESE FIRM’S GLOBAL DATA COLLECTION

THE WATCH STAFF

A leaked database shows a small company has collected personal data on 2.4 million people worldwide to feed intelligence to the Chinese government, media outlets reported in September 2020.

The data collected by Chinese firm Zhenhua Data includes addresses, birthdates, marital status, criminal records and political associations, *Forbes* magazine reported. It was largely harvested from social media profiles on Twitter, Facebook, Crunchbase, TikTok and LinkedIn. About 20%, however, comes from nonpublic sources. Only part of the database was recovered. It contains profiles of 52,000 U.S. residents, 35,000 Australians, 10,000 Indians, 9,700 Britons and 5,000 Canadians.

The data includes biographies and service records of U.S. Navy officers, including aircraft carrier captains. The firm also collected tweets from overseas U.S. military installations and social media chats among China watchers in Washington, *The Washington Post* newspaper reported. The information has been collected since 2017 for the stated purpose of providing intelligence to Chinese military, commercial and government clients, the *Post* reported.

The company left a copy of the database unsecured on the internet, where it was retrieved by an Australian cyber security consultancy.

Robert Potter, founder of the Australia-based Internet 2.0 cyber security company, and Christopher Balding, an independent researcher, provided an incomplete copy of the database to news organizations. Potter and Balding said they downloaded and reconstructed about 10% of the database, which is estimated to be about 1 terabyte of text. “Open liberal democracies must consider how best to deal with the very real threats presented by Chinese monitoring of foreign individuals and institutions outside established legal limits,” Balding said.



FIGHTING FOR THE TRUTH

**U.S. Global
Engagement
Center combats
disinformation
and propaganda**

THE WATCH STAFF

The United States Congress established the Department of State's Global Engagement Center (GEC) in 2017 to lead and coordinate interagency efforts to combat propaganda and disinformation from Russia, Iran, the People's Republic of China (PRC) and nonstate foreign terrorist groups.

With its new mandate and expanded resources, the GEC established threat teams, including a Russia Team, China Team, Iran Team and Counterterrorism Team. The GEC also created an Analytics and Research Team and a Technology Engagement Team to use the latest data analytics tools and technology to ensure success.

Propaganda is generally defined as the selective use of information, including false information, and the promotion of nonrational arguments for political effect. Disinformation is defined as the creation and dissemination of false content and/or manipulated information to deceive and mislead audiences.

Russia, the PRC, Iran and foreign terrorist organizations use propaganda and disinformation to mislead audiences, but they differ in their goals and tactics, according to the GEC's research and data science. For example, the Kremlin aims

to drive a wedge between the U.S. and its allies and partners and also to weaken democratic institutions. Its tactics include running long-term campaigns against targets while exploiting new opportunities presented by civil unrest and instability. Russia uses social media and unattributed websites to increase the reach of its disinformation and propaganda and to manipulate foreign audiences. Russia has expanded the scope of its targeting beyond Europe and the U.S. to include countries in Africa and Latin America.

Meanwhile, the Chinese Communist Party (CCP) seeks to shape the information space to its advantage. The CCP is pursuing a comprehensive and coordinated influence campaign to advance its interests and undermine those of the U.S., through a range of political, economic, military and information tools. Its propaganda apparatus is a critical component in promoting and maintaining the CCP's narrative domestically and globally. The CCP spends billions of dollars developing and expanding its international information infrastructure and the global footprint of its state-run propaganda machine. The CCP also exploits its economic influence to promote Beijing's global vision.



The Global Engagement Center was established in 2017 to fight foreign propaganda and disinformation.

GLOBAL ENGAGEMENT CENTER

For Iran, the main aim is advancing the regime's geopolitical goals across the Middle East and beyond. The Iranian government works to undermine U.S. policy and drive wedges between the U.S. and its allies by undercutting diplomatic and security partnerships. Conversely, it presents a false-positive image of events and circumstances within Iran. To advance its goals, Iran leverages a combination of traditional and social media.

Also of concern are violent extremist organizations (VEOs). They vary in their methods while vying for attention by amplifying shocking images or messages to recruit followers and/or undermine local security services. This differs from state actors, which work from a unified strategy with a set of coherent goals. Additionally, VEOs face logistical obstacles, often have less funding than state actors and have local law enforcement or other organizations working to thwart their efforts. VEOs tend to focus on spreading their ideology, recruiting members

and acquiring funding.

The GEC counters foreign propaganda and disinformation in various ways, including:

1. Using data analytics and technology to deepen its understanding of propaganda and disinformation campaigns.
2. Analyzing attempts by adversaries and competitors to target vulnerable foreign audiences, and sharing this information with partners and allies.
3. Building the technical skills of civil society and nongovernmental organizations, journalists and other local actors best positioned to expose and counter the spread of disinformation.
4. Partnering with diplomatic missions to share fact-based and historically accurate information via transparent mechanisms.
5. Building partnerships among U.S. government agencies, private industry, foreign allies and civil society.

HOW RUSSIA'S DISINFORMATION & PROPAGANDA

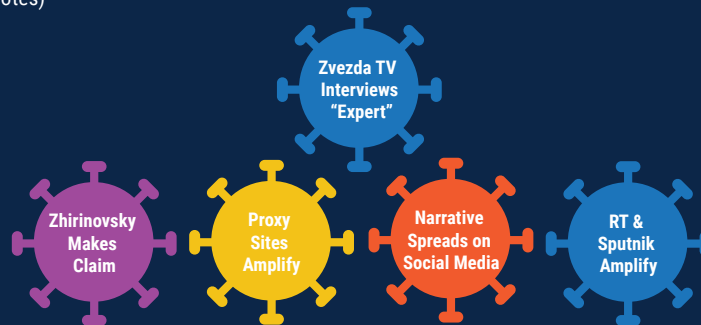


SPREADS

The Media Multiplier Effect
False Claim: The U.S. Created COVID-19

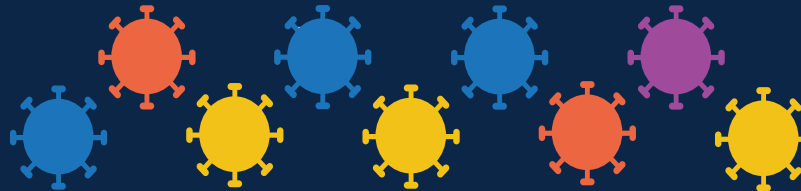
JANUARY 2020

Narrative begins. (see footnotes)



FEBRUARY 2020

The narrative begins to diffuse into the information environment.



MARCH-APRIL 2020

At this point, the narrative has fully diffused.



Footnotes:

Govorit Moskva: "[Russian politician] Zhirinovskiy calls coronavirus in China a biological weapon of the USA"

Zvezda TV: "An expert linked an outbreak of pneumonia in China with a biological weapon test."

Sputnik Arabic: "Is the Coronavirus a secret US biological weapon?"

Rossiya-1: "60 minutes in hot pursuit (evening release at 17:25) from 01.24.20"

News Front: "The new Chinese virus might be man-made: you need to close the American laboratory in Alma-Ata."

Geopolitica.ru: "Geopolitics of Epidemics: China and SARS Viruses"

Report: Digital Forensic Research Lab - Bioweapons, secret labs, and the CIA: pro-Kremlin actors blame the U.S. for coronavirus outbreak

Report: Mandiant Threat Intelligence - 'Ghostwriter' Influence Campaign'



PILLARS OF RUSSIA'S DISINFORMATION AND PROPAGANDA ECOSYSTEM



Official Government Communications

Kremlin or Ministry statement
Official Russian social media post
Statement or quote by Russian official



State-Funded Global Messaging

State-funded, foreign-facing media
State-funded, domestic-facing media
Foreign-based, Russian state-funded media
International Russian socio-cultural institutions



Cultivation of Proxy Sources

Russia-aligned outlets with global reach
Local language-specific outlets
Witting proliferators of Russian narratives
Unwitting proliferators of Russian narratives
Foreign state narrative amplification



Weaponization of Social Media

Infiltration of domestic conversations
Standing campaigns to undermine faith in institutions
Amplification of protests or civil discord



Cyber-Enabled Disinformation

Hack & Release
Site capture
Cloned websites
Forgeries
Disruption of official sources or objective media

CONNECTION TO RUSSIA



The GEC's Analytics and Research Team uses data analytics, message testing, subject matter expertise and public opinion polling to help its global network of partners counter foreign propaganda and disinformation. With this data, the GEC provides timely and actionable insights. Its analysis of social and online media data allows it to perform the critical task of identifying inauthentic activity on social media.

The GEC's data scientists and subject matter experts also have tracked state-sponsored disinformation campaigns related to COVID-19, which seek to exploit fear and uncertainty worldwide. Russian, Chinese and Iranian disinformation actors have promoted false narratives, including claims that the U.S. caused or exacerbated the pandemic.

Additionally, the GEC's Technology Engagement Team leads groundbreaking efforts to identify, test and implement new technologies against disinformation and propaganda. To date, the GEC has tested 20 unique technologies and shared this information on its platform, Disinfo Cloud. The GEC has over 200 tools under evaluation on Disinfo Cloud, which can be accessed by more than 1,100 technology experts and users.

The GEC's Technology Engagement Team also identifies new counter-disinformation technologies by hosting two-day Tech Challenges in partnership with foreign governments. For example, in 2019, Semantic Visions, a Czech Republic-based tool that enables counter-disinformation specialists to spot and assess emerging adversarial narratives online, won the Tech Challenge and was awarded funding.

Another vital element of the GEC's work is exposing the tactics of state actors and shining a light on nefarious activities. In August 2020, the GEC released the special report, "Pillars of Russia's Disinformation and Propaganda Ecosystem," as part of a U.S. government effort to help allies and partners understand and counter Russian disinformation campaigns. The report focuses on proxy sites, an often-overlooked part of the disinformation ecosystem. These sites play a significant role in elevating Russia's disinformation and propaganda because they appear to be independent and unconnected to Russia, lending credibility to the Kremlin-aligned disinformation they spread. The sites create and amplify Kremlin-aligned disinformation, which is then republished by other proxy and fringe sites, creating an echo chamber of disinformation.

The GEC also conceives and implements programs that raise awareness about state actors'

tactics to manipulate the information space. The programs include research that spotlights malign behavior; training for investigative journalists and fact-checkers; and public, fact-based messaging campaigns to inoculate vulnerable audiences against disinformation.

For example, the CCP seeks to acquire civilian research and technologies overseas to advance its military capabilities — a strategy known as military-civil fusion. In response, the GEC is supporting the Australian Strategic Policy Institute's efforts to use open source information to develop a comprehensive resource on the defense and security links of over 170 Chinese universities and research institutions. The project includes a public website accompanied by a report explaining the database's findings and

The GEC also conceives and implements programs that raise awareness about state actors' tactics to manipulate the information space.

recommending policies in response. The aim is to improve the ability of governments, universities and researchers to understand the potential risks of collaboration with the PRC and to raise the standard of universities' risk-management and due-diligence work.

To combat propaganda and disinformation threats from Russia, the PRC, Iran and foreign terrorist organizations, the U.S. and its partners and allies must work together. The GEC will continue to strengthen these partnerships, expose disinformation attempts by bad actors and push back against efforts to divide by building resilience to adversarial propaganda and disinformation. ▣



ARCTIC SECURITY: A CANADIAN PERSPECTIVE

**Nuanced
approach required
for defense,
safety, security**

DR. ADAM LAJEUNESSE AND DR. P. WHITNEY LACKENBAUER

Canada's 2017 defense policy — Strong, Secure, Engaged — depicts the Arctic region as “an important international crossroads where issues of climate change, international trade, and global security meet.” Changing physical and human geographies, new economic opportunities and the heightened interest of foreign state and nonstate actors are generating new security dynamics in the North American Arctic. While popular media typically depict contested boundary lines or the status of water disputes, Russian bombers entering airspace identification zones and a Russian military buildup in the Eurasian Arctic, most threats to Canada's North do not originate from Arctic conflicts.

Security threats are increasingly “all domain,” and the circumpolar region features great power competition in economic and military spheres, but military threats are not equally acute across all Arctic regions. For example, significant operational constraints remain in Canada's Arctic. Particularly in the maritime and land domains, environmental change is not opening the circumpolar North evenly, and not all threats are immune from physical geography. Canada's challenge lies in parsing which parts of the Arctic security environment and which regional dynamics or vulnerabilities require special or distinct analysis from more general national, continental and international defense preparedness and postures.

Canadian defense policy has evolved over the past 20 years to articulate a nuanced approach to Arctic security that spans the defense-security-safety mission spectrum. A careful assessment reveals that the most probable, short-term threats fall in the safety and secu-

urity categories. Canada's then-Chief of the Defence Staff Gen. Walt Natynczyk famously quipped in August 2009 that “if someone was foolish enough to attack us in the High North, my first duty would be search and rescue.” While such a pithy statement is excessively dismissive of Arctic threats that require a robust deterrence posture, it highlights how conventional military threats to the Canadian Arctic remain unlikely. Instead, Canada's Arctic strategies and operational planning documents over the past decade have appropriately emphasized comprehensive security, with the military playing a supporting role to civilian departments and agencies on most security and safety issues, such as pollution prevention, illegal immigration, poaching, environmental or humanitarian disaster and law enforcement.

Defense threats in the Scandinavian Arctic are naturally dominated by concerns over Russian militarization and aggression, while the Russian Arctic has seen a massive effort by Moscow to reestablish control and limit foreign access through a sophisticated effort known as anti-access/area denial. By contrast, the Canadian Arctic largely lacks military targets or critical infrastructure of strategic importance that, if destroyed or neutralized, would inhibit the ability of Canada or its allies to retaliate proportionately. Destroying or taking over North American Aerospace Defense Command (NORAD) forward operating locations or North Warning System stations would be a strong indicator that an adversary was planning a major offensive elsewhere and would surely invite Canada and its allies to respond. The cost-to-benefit ratio makes this highly unlikely except as a precursor to a major war.

HMCS Moncton passes an iceberg in the Arctic Ocean during Operation Qimmiq, which is a year-round surveillance patrol.

CPL. FELICIA OGUNNIYA/
ROYAL CANADIAN AIR FORCE



Increasingly, experts are downplaying the idea of state-based threats emanating from Arctic disputes, as political scientist Rob Huebert articulated in his “sovereignty on thinning ice” thesis in the 2000s. Instead, most current discussions emphasize the spillover of great power competition into the Arctic and the threat posed by strategic delivery systems that would transit the region to strike targets in the North American heartland. In this context, ballistic and cruise missiles, submarines and glide weapons are Arctic challenges because they pass through the region, but they have nothing to do with climate change opening access, competition over continental shelves or Arctic resources. Instead, these threats are best conceptualized through a wider international lens and the Canadian Arctic considered as a region in which to deploy sensors, ships and aircraft as part of a layered defensive ecosystem that will deter potential adversaries and defend the North American homeland as a whole.

Short- to medium-term foreign challenges to the Canadian Arctic are more likely to take the form of below-the-threshold operations, seeking to destabilize Canadian society by creating or exacerbating gaps and seams in social cohesion or long-standing alliances. To defend against these threats, intelligence analysts must be able to distinguish between legitimate forms of domestic democratic dissent and forms of meddling by nefarious actors. Furthermore, Canada must be highly attentive to trade-offs between the benefits of foreign investment that stimulates development and the security risks associated with a deeper foreign footprint in strategically significant locations. Ongoing debates about the People’s Republic of China’s expanding scientific interest and investment in Canada’s



Arctic and adjacent areas, particularly Greenland, are the clearest case in point.

While Chinese state-owned enterprises have funded strategic resource projects in the oil sands, the Arctic represents a different strategic landscape in several respects. If Chinese-backed resource projects represent the lion’s share of jobs and tax revenue in particular regions, will this give these projects — and by extension Beijing — disproportionate local influence and political leverage? Blocking such investment, on the other hand, risks setting the federal government against local communities seeking employment opportunities and new revenue streams through impact benefit agreements. Weighing risks and benefits, and countering disinformation and misinformation about these deals, will take on heightened saliency in the years ahead.

The emergence of new defense and security threats to the North American homeland is reigniting important discussions about where the Canadian Arctic fits. Moving beyond outdated “sovereignty on thinning ice” frames is essential for political support to deploy the right components of an integrated, layered defense ecosystem that is essential to defend our shared continent. Interoperability and information sharing between Canada and the United States, as well as other trusted allies and partners, is integral to future security. An essential precondition is that Canada is clear on what it is defending and against which type of threat.

Dr. Adam Lajeunesse is the Irving Shipbuilding chair in Canadian Arctic marine security at the Brian Mulroney Institute of Government, St. Francis Xavier University, Nova Scotia. Dr. P. Whitney Lackenbauer is a professor and Canada research chair in the study of the Canadian North at the School for the Study of Canada, Trent University, Ontario.



U.S. VIEW: EMERGING INFORMATION ENVIRONMENT

**Russia and People's Republic of China
demonstrate malign potential in Arctic**

TROY J. BOUFFARD AND DR. CAMERON D. CARLSON

Russia's top armed forces leader, Gen. Valery Gerasimov, authored an article in 2013 stating that the "role of non-military methods in achieving political and strategic goals has significantly surpassed the effectiveness of the power of weapons." His words came after the failed use of information operations (InfoOps) during the Orange Revolution in Ukraine in 2004 and the Russo-Georgian War in 2008. Russia refocused its InfoOps and executed a stunningly successful demonstration in Crimea during annexation in 2014, illustrating that strategic implementation of information warfare under relatively controlled circumstances represents a powerful approach.

The People's Republic of China (PRC) declared itself a "near-Arctic state" in the release of its Arctic strategy in 2018. While nearly a thousand miles from the region, the PRC seeks Arctic access and prominence through assertions such as economic development and climate research. Of Western concern is the growing Sino-Russian strategic cooperation that continues to deepen. For example, investments in and development of the Yamal and Arctic liquefied natural gas projects fuel the mutual economic interests of these great power competitors. Moreover, media and information coverage often strengthen adversarial legitimacy, providing the foundation to project power (and confusion). While the PRC may struggle to implement its 2018 Arctic strategy — especially the implied pursuit of increased access to the region — the information environment is wide open and ripe for Sino ascendancy.

In today's hypercommunicative world, the opportunity to leverage InfoOps can emerge almost spontaneously. Even when the occasion involves a fast-moving target,



As an emerging region of increased activity and vulnerability to information operations, the Arctic is primed for disinformation.

adversarial disinformation can be devastatingly effective. Such impacts generally rely on two requirements: 1) the disinformation content must be somewhat plausible, and 2) the initial outreach must be robust. Deterring attacks is a daunting task. The political and domestic attitudes concerning adversaries must be effectively aligned and consistent with national security priorities. Otherwise, divergent beliefs and perspectives within society could provide a landscape for adversaries to exploit. Developing a whole-of-government as well as a whole-of-society threat understanding is fundamental to developing disinformation resilience if only to avoid undermining efforts to counter disinformation. We need only remember the post-9/11 efforts in leading the United States to collective awareness and action concerning the threats posed by violent extremist organizations to the homeland.

Arguably, the most effective way to deter disinformation attacks involves reducing susceptibility and access to intended targets. Education is key: Rather than rely on defense or response to attacks as part of deterrence, develop a resilient society and government that is especially capable of absorbing and recovering from disinformation. Assisting society to recognize and verify questionable information is critical if for no other reason than to minimize our role as self-defeating accomplices. This aspect of InfoOps, as part of a broader national security element, is a capability that Russia and the PRC acknowledge to be just as, if not more, important as achieving supremacy in great power competition — something directly related to the PRC's One Belt, One Road goals or its Polar Silk Road policy.

As an emerging region of increased activity and vulnerability to information operations, the Arctic is primed for disinformation. The relative lack of Arctic understanding and attention for much of the U.S. allows for a more permissive environment from which malign interests could gain significant access and influence within our society. Other Arctic nations will also have to understand their information environments, especially as the circumpolar



Russian soldiers stand next to a military truck at the Russian base on Kotelny Island inside the Arctic Circle. AFP/GETTY IMAGES

nations depend on each other for mutual interests. For both Russia and the PRC, the number of targets and methods of disinformation delivery works to their advantage, especially when objectives can focus on domestic as well as multinational vulnerabilities. For example, much of the world has little understanding of the intensity involving northern Indigenous interests and geopolitics, which is as real and complex as any other sphere of power.

The U.S. must adapt to the globally unprecedented targeting power of social media (capability) and this pervasive form of subliminal interventionism (intent). The chance occasions to conduct InfoOps — planned or otherwise — become the other task as part of a timing game (opportunity), and thereby fulfilling the basic threat formula. Broadly, we can expect Russian InfoOps in the Arctic to involve geopolitical objectives while the PRC will likely focus on geoeconomic goals. However, all



A Russian soldier patrols the military base on Kotelnny Island. The base, dubbed the Northern Clover, is meant to serve as a model for military installations in the Arctic. AFP/GETTY IMAGES

Despite being nearly a thousand miles from the Arctic, the People's Republic of China has been seeking increased access to the region. Its second icebreaker polar research vessel, the Xue Long 2, launched in 2019. POLAR RESEARCH INSTITUTE OF CHINA



(overlapping) security sectors are exploitable, including political, military, economic, social and environmental. Western security concerns over Russian and Chinese goals involving the Arctic currently strive to delineate between real and perceived threats, which 1) remain potentially vulnerable to adversarial disinformation efforts, and 2) represent prospects to coordinate strategic and operational security-related miscalculations.

Militarily, the Arctic represents a traditional and new-generation threat to North America and the U.S. homeland. The information domain must seriously factor into defense thinking. Deterrence is considerably more difficult, simply because ideas cannot be killed and populations represent millions of participating information combatants, unwitting

or otherwise. While the Arctic remains a remarkable region of cooperation, Russia and the PRC will look to exploit the increasingly competitive realm of the circumpolar North in support of their global ambitions. To that end, vigilance remains vital. The U.S. government and society need to recognize the current level and usefulness of Arctic regional stability and leverage whatever time remains to prepare strategies against the malign disinformation endeavors of Russia and the PRC. ▣

Troy J. Bouffard is a faculty member at the University of Alaska Fairbanks and is a defense contractor with Alaskan Command, a joint subordinate unified command of U.S. Northern Command. He is also a research fellow at the Centre for Defence and Security Studies at the University of Manitoba. Dr. Cameron D. Carlson is program director for the homeland security and emergency management programs and is also the director of the Center for Arctic Security and Resilience at the University of Alaska Fairbanks.



BADGER, BEAR AND BISON INTERCEPTS

A history of
NORAD's
Russian
aircraft
intercepts

DR. BRIAN D. LASLIE

U.S. and Canadian fighter aircraft intercepting Soviet – and later Russian – bombers has long been a mainstay of the defense of North America. The cat-and-mouse game between the air forces of the Union of Soviet Socialist Republics and the combined air forces of Canada and the United States began before the North American Aerospace Defense Command (NORAD) officially started operations in May 1958. Soviet aircraft presented a threat to North America that needed to be countered.

The earliest visual contact with Soviet aircraft was recorded August 1, 1950. Two F-82 Twin Mustangs from the U.S. Air Force (USAF) 449th Fighter Interceptor Squadron were on a reconnaissance mission to photograph airfields in the Anadyr Gulf area of the Bering Sea. During this routine mission, the aircrews sighted four radial engine fighters in trail over an airfield. These were believed to be Soviet Lavochkin La-5, La-9 or La-11 aircraft, but no markings or insignia were observed. It was an inauspicious start to one of the Cold War's defining features.

The first U.S. encounter with Soviet MiG-15 jet aircraft took place March 15, 1953. While on a routine weather reconnaissance flight near the Kamchatka Peninsula, the crew of a WB-50 was fired upon by a pair of MiG-15s and returned fire. The encounter was about 100 miles east and slightly north of the Russian military base at Petropavlovsk. More important, the exchange was 25 miles out to sea over international waters. The Cold War was in danger of turning hot.

It was not until June 22, 1955, that interactions between East and West turned violent. At 11:09 a.m. local time, two Soviet jets fired on a U.S. Navy P2V over international waters in the Bering Strait. Only one U.S. crew member made a visual observation. As he watched the Soviet interceptors, one opened fire. The first burst set the port engine and fuel supply ablaze. A second severed the right wingtip of the U.S. aircraft. The pilot made a diving turn into a cloud bank 3,300 feet below and had no further contact with the lingering Soviet fighters. All 11 U.S. crew members survived, but several suffered burns from the attack and from a rough landing that caused a gas tank to burst. For the United States and Canada, the airspace between them and Russia was becoming a pivotal arena that required greater investment in defensive measures. These early tussles proved to be a driving factor in NORAD's creation.

The U.S. and Canada needed a mechanism to detect incoming Soviet aircraft. Defense agreements between the countries in the early 1950s centered on building radar networks across Canada – the Mid-Canada Line (also known as the McGill Fence), the Pinetree Line and the famous Distant Early Warning Line. This cooperation led to an extension of talks regarding the possible integration and execution of air defense plans. The Royal Canadian Air Force (RCAF) and USAF exchanged liaison officers and met at key conferences to discuss the potential of a shared air defense organization. By 1957, the details had been worked out, and each nation's top defense officials approved the formation



An F-14A Tomcat intercepts a long-range Soviet Tu-16 heavy bomber in 1985. NORAD



A U.S. Air Force F-14A Tomcat intercepts a Soviet Bison bomber in 1983. NORAD

of NORAD, which was stood up September 12, 1957, at Ent Air Force Base in Colorado Springs, Colorado. USAF Gen. Earle Partridge became NORAD commander and RCAF Air Marshal Roy Slemon, who was the key Canadian delegate in most of the cooperation talks, became deputy commander.

The nations announced eight months later on May 12, 1958, that they had formalized the cooperative air defense arrangements as a bilateral defense pact that became known as the NORAD Agreement. One of the key defensive mechanisms was the ability to intercept incoming Soviet bombers off the western coasts of Canada and the U.S.

Intercepts Begin

On March 5, 1958, radar tracked the first known Soviet long-range bombers flying a reconnaissance mission against U.S. forces in the Alaskan theater. Sixteen other such missions would take place through December 1961. The first recorded intercept of Soviet aircraft took place December 5, 1961. A pair of Tu-16 Badgers were intercepted off Alaska's northwest coast in the Bering Sea by two F-102s of the 317th Fighter Interceptor Squadron on alert at Galena airfield in Alaska. From that day to the end of the

Cold War in 1991, more than 300 successful intercept missions were flown against Soviet aircraft. In all, 473 Soviet aircraft were intercepted by aircrews from Alaskan Air Command and the 11th Air Force, as well as temporary duty aircrews from other commands and the RCAF. Not all intercepts were outside U.S. airspace. The U.S. Department of Defense first verified a Soviet flight over U.S. airspace on March 14, 1963, when two Soviet aircraft penetrated 30 miles into U.S. airspace over the southwestern corner of Alaska.

The Hunters and the Hunted

In the opening years of this Cold War confrontation, three types of Soviet bombers were intercepted near Alaska and the Aleutian Islands: Tu-16 Badgers, M-4 Bison and the infamous Tu-95 Bear. As technology progressed and the chilled conflict continued, other Soviet bombers joined the fold, including the Tu-22 Backfire and, toward the end of the Cold War, the Tu-160 Blackjack. These were matched by additions to the RCAF and USAF. The "hunters" included everything from F-47 Thunderbolts to century-series aircraft such as the CF-101 Voodoo, F-102 Delta Dagger, F-106 Delta Darts and F-4C Phantom II. New interceptors arrived in the



A North American Aerospace Defense Command F-22 Raptor intercepts a Russian Tu-142 bomber off the Alaskan coast in August 2020. NORAD



A North American Aerospace Defense Command CF-18 participates in an intercept exercise over Canada in March 2020.

CAPT. KYLE TUFTS/U.S. AIR NATIONAL GUARD

1970s and 1980s, including the F-15 Eagle. Today, NORAD uses the F-22 Raptor and the CF-18 Hornet.

Tu-16 Badgers were the only bombers intercepted between 1961 and 1968. The medium-range bomber could deliver nuclear or conventional free-fall bombs. That changed February 27, 1968, when two F-102s flying out of Eielson Air Force Base at Fairbanks, Alaska, intercepted three M-4 Bison strategic bombers over the Chukchi Sea. Developed in 1949 under the orders of Joseph Stalin, the Bison was the first Soviet bomber capable of reaching the U.S. The Bison entered service in 1955 and served as a bomber until the mid-1970s. The aircraft also was modified for inflight refueling and use as an aerial tanker. On April 10, 1983, F-15s intercepted two Bison over the North Pacific near the western Aleutians. Over 28 years, 111 Badgers in several variants were identified by U.S. pilots. The last Badger intercept occurred October 1, 1989, when two F-15s intercepted two Badgers in the North Pacific.

Badger and Bison intercepts were numerous, but by far the most regular appearance by Soviet bombers came in the form of the Tupolev Tu-95 Bear, which was intercepted 216 times by Alaska-based fighter aircraft. Since its introduction in 1954, virtually all variants of the Bear family of aircraft have been intercepted near Alaska. The first occurred February 16, 1968, when two F-106s on alert at King Salmon Air Force Station intercepted four Bears southeast of the Aleutians. The Bear H was the most hunted and prized Soviet aircraft for North American pilots. This included not only the USAF and RCAF, but also the U.S. Navy. In 1987, two F-15s from King Salmon and two F-14s from Adak Naval Air Station conducted the first interservice intercept of two Bear Hs. However, by the late 1980s, Soviet long-range flights had dropped off precipitously and ended almost entirely with the collapse of the Soviet Union and the end of the Cold War.

Russian Long-Range Aviation

With hindsight, it becomes clear that the Soviet Union's collapse offered only a brief respite in intercepts. In 1992, NORAD completed a strategy review, which documented the wide-ranging changes in the security environment since the close of the Cold War. The report noted the need for air sovereignty, warning and assessment, as well as the potential need to better integrate a ballistic missile defense mission. In short, the report provided a baseline for the command's continued existence. Although the Soviet Union no longer posed a threat, its successor states still had air- and submarine-launched cruise missiles. Russian aviation was down but not out.

By 2014, Russian long-range aviation and maritime activity reached levels not seen since the Cold War. Russia was conducting more sorties, supported by more tankers, and establishing more sophisticated linkages between air and maritime intelligence collection than ever before. This activity underscored an aggressive Russian military enjoying new prosperity, proficiency and ever-improving capabilities that had NORAD focused on the Russian Bear once more. NORAD's three operational regions in Alaska, Canada and the continental U.S. routinely responded to Russian long-range aircraft entering the North American Air Defense Identification Zone. For example, on July 4, 2015, NORAD fighters intercepted two Bear bombers west of Alaska's coast and off the coast of central California.

Intercepting Russian long-range aircraft continued through 2020. Much like the pilots of the early Cold War, U.S. and Canadian Airmen remain ready to play the dangerous game of cat-and-mouse with a new generation of adversaries.

Dr. Brian D. Laslie is the deputy command historian for U.S. Northern Command and the North American Aerospace Defense Command.

BUILDING RESILIENCE

THE WATCH STAFF

U.S., allies face tests posed by technology and great power rivals

Great power adversaries of the United States — the People’s Republic of China (PRC) and Russia — are pursuing multiple strategies to undermine the sense of security that oceans of distance once afforded defenders of North America. Both countries are developing hypersonic weapons that can reach the U.S. and travel at more than five times the speed of sound. The PRC is investing in the infrastructure of nearly 70 countries worldwide through its One Belt, One Road (OBOR) program, giving it political influence and access to deep-water ports from which to project power. These adversaries are even trying to undermine U.S. security by gaining footholds in the northern approaches to the continental U.S. by investing in the Arctic.

The security threats extend beyond conventional military calculus. An onslaught of cyber intrusions and supply chain shortages during the coronavirus pandemic tested the resilience of the U.S. and its allies. The diverse and complex challenges posed by this new era of great power competition have defense experts calling for the strengthening of national resilience to become a pillar of U.S. homeland defense strategy. “The enormous challenges presented by the [COVID-19] virus are reflective of a broader spectrum of resilience risks facing the United States,” wrote Franklin D. Kramer in an October 2020 report for the Atlantic Council. Kramer was a senior appointee in two U.S. administrations, including as assistant secretary of defense for international security affairs.

“Since the turn of the century,” he wrote, “three converging factors — the ever-increasing reliance on information and communications technology, the globalization of supply chains, and the rise of China as a competitor — have created vulnerabilities that have put the United States at increasing risk. Along with the biological and health risks that the pandemic has exposed, these vulnerabilities call for an expanded focus on resilience as a key element of U.S. strategy.”

Kramer’s report, “Effective Resilience and National Strategy: Lessons from the Pandemic and Requirements for Key Critical Infrastructures,” identifies vulnerabilities ranging from China-centric supply chains to exploitable cyber systems. The road to a resilient society, he contends, requires a combination of diplomacy, economic cooperation between the public and private sectors and military deterrence to harden the homeland defense shell.

CYBER SOFT SPOTS

Recent reports underscored cyber vulnerabilities. The U.S. Department of Homeland Security and the Federal Bureau of Investigation (FBI) issued a joint alert in May 2020 “warning organizations researching COVID-19 of likely targeting and attempted network compromise by the People’s Republic of China (PRC).” Health care, pharmaceutical and research companies working on the COVID-19 response “should all be aware they are the prime targets of this activity and take the necessary steps to protect their systems,” the warning stated.



The U.S. investment in Greenland is significant, analysts said, because it signals an intention to gain a foothold in the Arctic and take advantage of sea routes that are opening as polar ice caps melt.

The icy shores of Greenland are attracting the interest of the People's Republic of China and the United States as resource-rich waters and vital shipping routes become key components of great power competition.

AFP/GETTY IMAGES



The Vladimir Rusanov, a liquefied natural gas tanker, docks at a terminal in eastern China's Jiangsu province after its journey from Russia's Yamal Peninsula. Russia and the People's Republic of China are partners in a liquefied natural gas plant in the Siberian Arctic.

AFP/GETTY IMAGES

The agencies concluded: “China’s efforts to target these sectors pose a significant threat to our nation’s response to COVID-19.”

Calling the PRC the greatest counterintelligence threat to the U.S., FBI Director Christopher Wray told the U.S. Senate Homeland Security and Governmental Affairs Committee in September 2020 that Chinese hackers continue to target U.S. firms working on coronavirus vaccines, treatments and testing technology. “Sometimes, without being too descriptive in an open setting, we can almost track a news report from some company or research institution that is announcing or revealing some progress ... and then almost within days we will see cyber-targeting that ties back to Chinese actors focusing on those institutions,” he said.

The nature of an ever-changing cyber environment creates vulnerability, Kramer wrote. Unlike a physical system that is rarely modified after production, software is subject to continual revision through updates and patches. “This makes the supply chain for code long and subject to myriad flaws, both unintentional and malicious,” his report states.

He recommends that “cyber security resilient architectures” be developed for the key sectors of energy, finance, food, health, transportation and the defense industrial base, with federal funding provided to support the development and operation of these cyber defenses. The U.S. Congress, Kramer recommends, should enact

legislation to establish a research and development strategy that would lead to the creation of resilient cyber infrastructures for critical industries.

PROMOTING ACADEMIC RESILIENCE

Building resilience is a huge challenge for academia. The U.S. university system through its “wellspring of ideas, experimentation and talent played a signature role in ending World War II and buttressing the space program in the 1960s,” said an April 2020 report published by the Brookings Institution titled, “Preparing the United States for the Superpower Marathon with China.” The report by scholars Michael Brown, Eric Chewning and Pavneet Singh states that since the fall of the Berlin Wall in 1989, the national purpose that motivated professors and students to tackle complex security challenges has faded. The PRC now graduates six to eight times as many science, technology, engineering and mathematics (STEM) students than the U.S. “University programs are financially strained and must seek higher-paying foreign students — often Chinese nationals — to fill the ranks. But the U.S. immigration system does not allow these students to stay in the U.S. after graduating. So not only are U.S. taxpayers subsidizing the education of foreign talent in advanced STEM fields, we are subsequently losing the potential economic benefits of that investment,” the report states.



Hackers from the People's Republic of China have attempted to steal vaccine and testing technology from U.S. companies working to defeat the coronavirus.

AFP/GETTY IMAGES

The brain drain is damaging U.S. resilience in a key area of intellectual pursuit. Cash-strapped universities are exploring partnerships with foreign funding sources, often Chinese, the report states, adding: "These soft power tools are not benign in their motivations and have been often documented to be vectors for propaganda."

The authors suggest that one way to establish resilience in STEM fields would be to make a "generational commitment" to STEM education. The U.S. government, they contend, should provide financial incentives for students to study STEM fields and offer government internships that lead to employment. Also needed are corporate tax credits for companies to hire more engineers and partial student-loan forgiveness for STEM students, the authors say.

UNEVEN PLAYING FIELDS

Another key test of resilience is the pressure of competing in a global economy where others don't play by the same rules. The PRC and Russia blur the lines between "economic and national security, exerting state control over economic assets to further their national interest,"

the Brookings report authors note. That leaves many U.S. companies outmatched when competing against state-subsidized firms such as those in China.

The challenges require the U.S. to look beyond a pure military analysis, whether about the inventory of aircraft carriers or the number of special operations forces in a theater, to assess the readiness of homeland defense, the authors contend. "The solution sets should instead integrate economic and financial tools such as sanctions, market access, and export controls along with forward military deterrence."

Congress will rally behind U.S. businesses and research and development efforts, the authors contend, as will other nations if the U.S. takes the lead in building markets and supply chains that aren't reliant upon the PRC. "Given China's growing economy, investment in science and technology, and coercive power over its people, the winner of this superpower marathon is by no means certain," the authors state. "The stakes, however, are paramount given China's ideological differences and technology capability fueling an economy that is on a path to eclipse our own."

ARCTIC CHESS MATCH

Perhaps nowhere is the challenge to U.S. resilience greater than in the Arctic, where the PRC and Russia have focused attention to control lucrative shipping routes and natural resources. The stakes in this contest involve key diplomatic, economic and military endeavors.

In April 2020, two Russian companies announced an agreement to build the world's most powerful nuclear icebreaker, which Russia hopes will drive open shipping routes. The deal was unveiled about the time the U.S. announced increased financial investment and diplomatic efforts in Greenland to combat Chinese influence. The U.S. announcement occurred as two Chinese icebreakers returned home after a six-month Arctic deployment.

The U.S. investment in Greenland is significant, analysts said, because it signals an intention to gain a foothold in the Arctic and take advantage of sea routes that are opening as polar ice caps melt. Mineral-rich Greenland, the world's largest island, is strategically located between North America and Europe. Most of the U.S. \$12.1 million in aid will be in the form of U.S. advisory and consultancy services, used to "benefit the economic development of Greenland, including the mineral industry, tourism and education," according to a statement by the Greenlandic government. The U.S. also opened a consulate in Greenland.

Chinese leaders are increasingly interested in the Arctic and declared their country a "near Arctic nation," a designation rejected by the international community. They also have discussed plans for a "Polar Silk Road" as an extension of the OBOR infrastructure program. Proposed Chinese projects in Greenland include building a research station, establishing a satellite ground station and improving airfields. The recent Sino-Russian cooperation in the Arctic signals a new challenge for the U.S. and its allies and a heightened test of U.S. resilience.

A June 2017 policy paper by the Stockholm International Peace Research Institute suggested that the PRC and Russia were already beginning to collaborate with frequency in the Arctic, mainly because Russia's natural resources are becoming exploitable, thanks to Chinese investment. "The sanctions imposed on Russia by Western states following the annexation of Crimea have, however, significantly restricted Russia's ability to access the capital and technology necessary to develop its far northern territories," the paper states. "Determined to push ahead with the development of the Arctic, Russia has looked elsewhere for investment, notably to China."

The challenge for the U.S. and its allies is to develop a resilient and consistent Arctic strategy — diplomatic, economic and military. Military leaders have argued for a greater Arctic presence. "Without presence, diplomacy and cooperation are absent or empty," Adm. Karl L. Schultz, commandant of the U.S. Coast Guard, said at a December 2018 forum hosted by the Wilson Center. "Without presence, our regulatory roles, our governance,

Threats to U.S. security are global and originate across all sectors — from industry to health care to the military.



and international agreements become hollow policies. In the Arctic region, presence equals influence. The truth is, if we aren't present, if we don't know the environment today, our competitors will."

RESILIENCE AS A STRATEGY

To make a country resilient in the face of great power competition requires military deterrence in conjunction with coordinated statecraft and economic initiatives, Kramer argued in his report for the Atlantic Council. U.S. Northern Command (USNORTHCOM) and the North American Aerospace Defense Command (NORAD) are investing in systems powered by artificial intelligence and machine learning to provide better early detection of conventional missiles and deliver a quicker and more complete picture of all warfighting domains. NORAD and USNORTHCOM also routinely provide deterrence by intercepting long-range Russian bombers and participating in air intercept and quick deployment exercises in the Arctic.

Threats to U.S. security are global and originate across all sectors — from industry to health care to the military. "Our homeland is not a sanctuary," wrote U.S. Air Force Gen. Glen D. VanHerck, commander of USNORTHCOM and NORAD, in a newsletter to his commands. "These words are inscribed over the entrance to our headquarters and remain a guiding principle for our commands as we continue to defend our homelands." ▣



Green Berets with the 10th Special Forces Group (Airborne) offload their vehicles in Deadhorse, Alaska, after deploying as part of an exercise to defend against threats to oil fields.



Green Berets maneuver through Deadhorse, Alaska.

ARCTIC SUCCESS

SPECIAL FORCES DEPLOY TO ALASKA TO SIMULATE OIL FIELD DEFENSE

Story and photos by 10TH SPECIAL FORCES GROUP
(AIRBORNE) PUBLIC AFFAIRS OFFICE

Editor's note: The names of those serving in the 10th Special Forces Group (Airborne) are withheld for the safety of the Soldiers and their families.

Special Operations Command North (SOCNORTH) teamed up with Air Mobility Command to deliver a tailored special operations task force north of the Arctic Circle on minimal notice in September 2020.

SOCNORTH deployed a task force composed of a crisis response force planning element and a Green Beret team from the 10th Special Forces Group (Airborne) to confront a simulated threat from a terrorist group to Alaskan oil production.

The SOCNORTH team, an advanced command and control element, coordinated with civil authorities while the Green Berets conducted reconnaissance to provide an operational understanding for possible follow-on forces.

"The intent here is to ensure that we are all trained and able to

leave on a moment's notice to get on an aircraft across the city, load up and head to wherever the mission takes us," said the 10th Special Forces Group's detachment commander.

Established after 9/11, SOCNORTH's primary mission is anticipating and planning for threats to the homeland.

The Arctic is rapidly gaining in strategic importance as a source of fossil fuels and maritime passage. Alaska, Canada and Russia account for nearly 10% of the world's oil reserves, with the Alaskan Arctic holding the largest volume, according to the U.S. Geological Survey.

The task force transported all-terrain vehicles and a command and control vehicle to the Arctic from Peterson Air Force Base in Colorado Springs, Colorado, aboard a C-130J Hercules aircraft.

Mission planners highlighted the mobility challenges of working in the Arctic in the transition period between summer and winter, when daily temperatures typically average 27 to 37 degrees Fahrenheit.

"We've performed this mission before in the middle of winter, when the chief concern is the deep negative temperatures," said the lead mission planner from U.S. Special Operations Command. "But, in a way, that makes the terrain easier as it's frozen solid and snow machines have no issues."

Mobility in September is a different story, he said, because the region has few maintained roads and the daily freeze-thaw cycle turns open terrain into variable marshland.

The largely flat region makes it challenging to find vantage points for reconnaissance, the planner said.

A substantial success of the exercise was that the team established direct communications with its Colorado Springs headquarters using high-frequency radio over a distance of more than 2,600 miles.



Green Berets and Special Operations Command North personnel establish communications from the Arctic to command headquarters in Colorado Springs, Colorado.

RETHINKING SUPPLY CHAINS

Pandemic Exposes Weaknesses in China-Centric Processes

INDO-PACIFIC DEFENSE FORUM



The coronavirus pandemic that infected more than 108 million people worldwide by mid-February 2021 laid bare more than the grocery store shelves ravaged by panicked buyers from Texas to Tokyo. The manufacturing lockdown in the People's Republic of China (PRC) caused by the spread of COVID-19 exposed critical weaknesses in supply chains that left U.S., European and Indo-Pacific leaders searching for products ranging from personal protective equipment to pharmaceuticals. It also prompted a call to action: Build supply chain resilience to keep history from repeating itself.

The eye-opening shortages of the pandemic are spurring calls for new partnerships. The United States is pushing to create an alliance of partners dubbed the Economic Prosperity Network, which would include companies and civil society groups operating under a single set of standards on everything from digital business and energy to research, trade and education, Reuters reported.

The U.S. wants to work with Australia, India, Japan, New Zealand, South Korea and Vietnam to “move the global economy forward,” then-U.S. Secretary of State Mike Pompeo said in April 2020, according to Reuters. The discussions include “how we restructure ... supply chains to prevent something like this from ever happening again.”

A key plank in the U.S. economic security strategy is the expansion and diversification of supply chains that protect “people in the free world,” according to Keith Krach, a State Department official who leads efforts to develop international economic growth policies. Krach

said the Economic Prosperity Network would be built for critical products such as pharmaceuticals, medical devices, semiconductors, automobiles, textiles and chemicals.

RARE-EARTH CHALLENGES

The PRC has a chokehold on the global market for rare-earth minerals, which are used in everything from advanced weaponry to computers and smartphones. It produces about 70% of the world's rare-earth exports, thanks to 15 years of industrial policy in which the government invested in building companies and subsidizing production to undercut competition, according to a September 2020 Bloomberg article by four defense scholars, including former U.S. Defense Secretary James Mattis.

U.S. military and commercial supply chains are almost solely dependent on the PRC for rare-earth minerals, but this is a fixable problem, the scholars noted.

The U.S. government already is making long-term investments. The minerals were not mined in the U.S. as recently as 2017, the Bloomberg article noted. With Department of Defense support to reopen the Mountain Pass Mine in Southern California, however, the U.S. now provides 12% of the global supply of unprocessed rare-earth minerals. The U.S. is also planning to open mines in Nebraska, Texas and Wyoming, as well as a pilot processing plant in Colorado. “If the U.S. is able to solve the problems posed by Chinese domination of rare earths,” the defense scholars noted, “it could provide a model for building greater resilience in American and Western supply chains more generally.”





INDO-PACIFIC NEIGHBORS SEEK CHANGE

The PRC's neighbors also want more resilient supply chains. "We have become dependent on China," Japanese Economy Minister Yasutoshi Nishimura told Reuters in June 2020. "We need to make supply chains more robust and diverse, broadening our supply sources and increasing domestic production." Officials in India, Singapore and Taiwan echoed his sentiments as governments began analyzing supply chain resilience and, in some cases, providing subsidies to companies willing to relocate.

In Japan, then-Prime Minister Shinzo Abe launched a U.S. \$2 billion program in April 2020 to provide stimulus funds to help companies shift production home. Some government officials in Tokyo deemed the need to diversify the supply chain a matter of national security. Although the pandemic provided fresh evidence of supply chain vulnerabilities, Japanese leaders have been talking about the need to build resilience since the early 2000s, when the cost of Chinese labor started to soar, Reuters reported. Those cost increases sparked discussions in Japan of a "China plus one" strategy — a policy of managing risk by situating plants in the PRC and at least one other Indo-Pacific country.

"Many companies have already begun adopting a China plus one manufacturing hub strategy since the U.S.-China trade war began in 2018, with Vietnam having been a clear beneficiary," said Anwita Basu, head of Asia country risk research at Fitch Solutions, according to a June 2020 report by Bloomberg. Although the pandemic will continue that trend, "shifts away from China will be slow as that country still boasts an annual manufactur-


ing output that is so large that even a group of countries would struggle to absorb a fraction of it."

Still, Indo-Pacific industries and governments see the perils of overreliance on their larger neighbor. Taiwan officials in 2019 encouraged companies on the island to build a "non-red supply chain" outside mainland China. They approved laws that provided low-cost loans, tax breaks, rent assistance and simplified administration to companies that invested in Taiwan. A major development in the supply chain reshuffle occurred in May 2020 when one of the world's leading computer chipmakers, Taiwan Semiconductor Manufacturing Co., said it would build a U.S. factory in Arizona.

Singapore, meanwhile, has also been promoting the need to diversify. Singaporean Trade Minister Chan Chun Sing said the pandemic's paralyzing effect on supply

"Many companies have already begun adopting a China plus one manufacturing hub strategy since the U.S.-China trade war began in 2018, with Vietnam having been a clear beneficiary."

*~ Anwita Basu,
head of Asia country risk research,
Fitch Solutions*



Flight cadets from all branches of the Indian Air Force Academy wear face masks during a graduation parade. Shortages of face masks and other personal protective equipment were reported worldwide when China shut down manufacturing plants.

AFP/GETTY IMAGES



chains has been eye-opening. “Today, China is not just producing low-end, low-value products. They are also in the supply chains of many of the high-end products. And that means that the impact on the supply chains will be significant across the entire globe,” he told CNBC’s *Squawk Box Asia*.

For essential items, Singapore “will carefully build up some local capacities that we can surge in times of need,” Chan said, according to *The Straits Times* newspaper. That includes looking at “where the goods come from, where the manpower comes from, which market supplies to us” and even which shipping line brings the goods into Singapore.

China-centric supply chains aren’t the only concern, he pointed out. Singapore has diversified its rice supply, which in the past mostly came from Thailand and Vietnam. Now, Singapore also gets rice from Japan and India, he added.

The sheer volume of companies dependent on Chinese manufacturing illustrates the need for alternatives. A March 2020 analysis published by the *Harvard Business Review* magazine noted that the world’s largest 1,000 companies or their suppliers own 12,000 facilities — factories, warehouses and other operations — in COVID-19 quarantine areas of the PRC, Italy and South Korea.

Companies worldwide scrambled to identify which of their invisible suppliers — those with whom they don’t directly deal — were based in the affected regions of the

Employees check the quality of face masks produced at the Thai Nguyen Garment factory in Vietnam. Vietnam has become an attractive alternative for global companies wanting to build supply chain resilience. AFP/GETTY IMAGES

PRC, the analysis stated. “Many companies are probably also regretting their reliance on a single company for items they directly purchase. Supply-chain managers know the risks of single sourcing, but they do it anyway in order to secure their supply or meet a cost target,” the article stated. “Often, they have limited options to choose from, and increasingly those options are only in China.”

DIVERSIFICATION BRINGS OPPORTUNITY

As global companies build supply chain resilience, Indo-Pacific nations stand poised to reap the benefits. Indian Foreign Secretary Harsh Vardhan Shringla said in a June 2020 speech that countries “will be looking for maximum diversification of their production and supply chains in the medium to long term, weaning away from extreme dependence on any one particular country or region,” according to a report in *The Economic Times* newspaper.

India, he added, has the opportunity to develop itself into a low-cost manufacturing hub. He said companies could pinpoint shortfalls in supply chains sooner if they worked with India, which has highly functioning democratic systems and higher levels of transparency

than the PRC.

India plans to focus some of its manufacturing efforts on pharmaceutical ingredients to become an alternative supplier for drugmakers affected by factory shutdowns in the PRC, Bloomberg reported. The Indian government, the report said, wants to identify essential drug ingredients, provide incentives to domestic manufacturers and revive ailing state-run drug companies.

India, which is the world's largest exporter of generic drugs, experienced raw material shortages caused by the coronavirus outbreak, signaling its dangerous dependence on the PRC for those supplies. India imports almost 70% of the chemicals it uses to make generic drugs from the PRC. Some of these sources are in Hubei province, where the coronavirus outbreak emerged in December 2019.

To kickstart the supply chain overhaul, the Indian government established a U.S. \$1.8 billion fund in March 2020 to set up three drug manufacturing hubs, and identified 53 key starting materials and active pharmaceutical ingredients that would be made a priority. These include the fever-reducing medicine paracetamol and antibiotics that include penicillin and ciprofloxacin.

India isn't the only Indo-Pacific nation looking to become an integral part of global supply chains. Low-cost labor and low land prices have long paid dividends for Vietnam as companies a few years ago started relocating their manufacturing sites outside the PRC. The global pandemic will do nothing to slow that trend, according to an April 2020 report from Jones Lang LaSalle (JLL), a U.S.-based global real estate consultancy.

U.S. Census Bureau data, for example, showed a nearly 36% surge in goods imported into the U.S. from Vietnam in 2019 compared with a 16.2% contraction in goods imported from the PRC. "Data for this year will be distorted by the effects of the coronavirus on global supply chains, but the trend of manufacturing moving from China to Southeast Asia will continue," said Stuart Ross, JLL's head of industrial and logistics for Southeast Asia.

GETTING UNTANGLED

Chinese manufacturing is so deeply woven into the fabric of international supply chains that diversification and resilience building in Indo-Pacific countries won't happen overnight. Japan is a good example. The government's U.S. \$2 billion program to lure companies into domestic production is a start, but Japanese companies are deeply invested in Chinese manufacturing hubs. Japanese companies had at least 7,400 affiliates in the PRC as of March 2018, according to a Trade Ministry survey, Reuters reported. That number is up 60% from 2008.

The development of more automation and the onset of artificial intelligence-based technology could be one of the answers to developing more supply chain resilience. Japan Display Inc. and chipmaker Rohm Co. Ltd. told Reuters that potential shifts to full automation for



A customer purchases generic medicine from a pharmacy in New Delhi, India. India is investing in its pharmaceutical supply chain to lessen its dependence on China.

AFP/GETTY IMAGES

The development of more automation and the onset of artificial intelligence-based technology could be one of the answers to developing more supply chain resilience.

labor-intensive, back-end processes could lead to new assembly lines being built in Japan.

For others, however, the PRC will remain in their supply chains for cost reasons. Sharp Corp., which makes display panels and televisions, ships products to the PRC where backlights, connectors and other parts are added. The process requires manual testing and machinery adjustments. "The back-end process has long been done in China because it's labor-intensive," said a spokesman at Sharp, which was acquired by Taiwan's Foxconn in 2016. "It would be expensive to bring it back home."



A WAY FORWARD

Supply chain experts point out that the PRC engineered its manufacturing advantage by creating a supply chain network that is bolstered by a vast distribution system and efficient transportation infrastructure. It also offers a large pool of workers who are trained in operating complex machinery. As firms reexamine their supply chains in a post-pandemic economy, the “pressure from governments to re-shore operations versus the attractiveness of China as a manufacturing hub will be a persistent geo-economic tension they will have to navigate,” according to an article published by Yoganathan S/O Theva, an associate research fellow in the Policy Studies Group at the S. Rajaratnam School of International Studies, Nanyang Technological University, in Singapore.

To navigate a post-coronavirus economy, he argued, “firms should avoid a rigid, binary approach of completely relying [on] or decoupling from China. Instead, firms should pursue supply chain resilience by being nimble and strategically switching their operations between China and other countries when needed.”

Strategies to achieve this, he said, could include investments in building multisource supply chain networks and

creating circular supply chains that enable companies to reuse discarded materials. Global companies also need maximum visibility on their supply chain networks to anticipate disruptions emanating from the PRC or elsewhere, he said.

To achieve this visibility, companies such as Corning, Emerson, Hayward Supply and IBM are using digital technologies such as blockchain to create a reliable audit trail that tracks an asset from production to delivery. “Armed with such data, firms will be able to quickly identify the specific supply chains that will be disrupted and activate alternative supply chains,” Theva wrote.

Whether decoupling completely from the PRC or simply diversifying supply chains to build resilience, Indo-Pacific industry leaders agree that the status quo of heavy dependence on Chinese manufacturing needs to be addressed. “Everyone agrees we really have to reconsider the sustainability of supply chains,” Hiroaki Nakanishi, chairman of Hitachi Ltd. and head of Japan’s biggest business lobby, said in a May 2020 televised interview. “It’s unrealistic to suddenly return all production to Japan. But if we are totally reliant on one specific country and they have a lockdown, there will be huge consequences.” ☐

AGILE AND ON GUARD

NORAD hones air defenses, readiness with Arctic exercise

THE WATCH STAFF

Ongoing threats from great power competitors are placing ever-greater importance on military exercises by Canada and the United States that stress troop readiness and air defense capabilities as the mission of protecting the approaches to North America becomes increasingly complex.

The binational North American Aerospace Defense Command (NORAD) conducted Operation Noble Defender in the Arctic in September 2020 as Russian military incursions along the periphery of Canada and the U.S. persisted. “As competitors seek to bolster their presence and increase military operations in the Arctic, NORAD remains vigilant and ready to protect the sovereign airspace of Canada and the United States to detect, deter and defeat potential threats to our air and maritime approaches,” NORAD Commander Gen. Glen D. VanHerck said in a statement.

The operation spanned all three NORAD regions — Alaska, Canada and the continental U.S. F-22, CF-18 and F-16 fighter aircraft conducted air defense operations with support from an E-3 Airborne Warning and Control System (AWACS) aircraft, and KC-135 and CC-150T refueling tankers. The exercise demonstrated agile and dynamic force employment to and from critical forward-operating locations along North America’s northern approaches.

“Coordinated and partnered binational operations such as this are vital to the continued defense of North America,” said Maj. Gen. Eric Kenny, commander of the Canadian NORAD region. “This extensive operation shows the iron-clad relationship that exists within the NORAD team. We stand ready to deter and defeat threats along our approaches.”



Senior Master Sgt. John Rohrer, a public affairs superintendent from the Colorado Air National Guard, shares his imagery with pilots and crew during Operation Noble Defender in the Arctic in September 2020. CAPT. CAMERON HILLIER/U.S. AIR FORCE

The need to hone these capabilities came into sharp focus just two days before the exercise began. NORAD F-22 Raptors and an E-3 AWACS aircraft, which were supported by KC-135 refuelers, identified two Russian Tu-160 bombers and two Su-35 fighter aircraft that entered the Alaskan Air Defense



Identification Zone (ADIZ) three times on the night of September 18, 2020.

The Russian aircraft loitered in the ADIZ for a total of about four hours, NORAD reported, and came within 50 nautical miles of Alaska's Nunivak Island. They remained in international airspace and did not enter U.S. or Canadian sovereign airspace.

"The re-emergence of strategic competition between nations, and competitors who overtly challenge the free and open international order, characterizes our complex global security environment," VanHerck said, according to a NORAD news release.

HARDENING THE SHIELD

NORAD employs a layered defense network of radars, satellites, and fighter and early warning aircraft to identify aircraft and determine appropriate responses. The identification and monitoring of aircraft entering the ADIZ of Canada or the U.S. demonstrates how NORAD executes its aerospace warning and control missions.

Repeated encounters with Russian aircraft near North America call for more than regular exercises to sharpen readiness. They also signal a need to upgrade NORAD's early warning system, according to current and former NORAD leaders.

Brig. Gen. Pete M. Fesler, deputy director of operations for NORAD, and then-NORAD Commander

Gen. Terrence O'Shaughnessy published a paper in September 2020 for the Wilson Center titled "Hardening the Shield: A Credible Deterrent and Capable Defense for North America." The paper illustrates the threat of "horizontal escalation," a tactic designed to incapacitate North American militaries before they can mobilize. Russia and the People's Republic of China (PRC) are developing long-range conventional weapons designed to strike soft economic targets inside North America, such as ports and airports, the generals wrote.

In Russia's case, "Tupolev bombers and ultra-quiet, nuclear-powered submarines now frequently conduct mission rehearsals for strikes on the United States and Canada" in areas beyond NORAD's radar coverage, they warn. "This is not messaging," the paper continues. "The Kremlin's stealthy operations are designed specifically to remain undetected, and what good is a strategic message if it is not received?"

NORAD is developing a data-driven, machine learning system called the Strategic Homeland Integrated Ecosystem for Layered Defense (SHIELD). The system analyzes data and extrapolates it into a common operational picture, Fesler told an online forum. "It scans the data for patterns that are not visible to human eyes, helping decision-makers understand adversary potential courses of action before they are executed," Fesler and O'Shaughnessy wrote.



A member of the Royal Canadian Air Force guards an F-16 Fighting Falcon before the start of Operation Noble Defender.

SENIOR MASTER SGT. JOHN ROHRER/
COLORADO AIR NATIONAL GUARD



CF-18 Hornets prepare to refuel over Canada's Labrador region during Operation Noble Defender.
CAPT. CAMERON HILLIER/U.S. AIR FORCE

CHANGING SECURITY ENVIRONMENT

Technological superiority is a must for homeland defenders who operate in an increasingly contested environment. U.S. adversaries learned from wars in which the U.S. and its allies won on the battlefield, the generals wrote, and designed strategies and systems “intended to circumvent the military strength of the West.”

“Today, the oceans that were formerly the moats that defended the arsenal of democracy have become a means of approach, the Arctic is no longer an icy fortress wall protecting the northern flank, and the skies in which American airmen operated with impunity for the last three decades have become contested and the preferred domain for adversary kinetic attacks on the homeland,” Fesler and O’Shaughnessy wrote.

If the traditional U.S. warfighting method is to deploy overwhelming force overseas, “then the way to defeat the United States military in the next war, in the minds of her adversaries, is to prevent deployment in the first place.”

Threats to the homeland are growing. Over the past decade, China’s People’s Liberation Army (PLA) has fielded an array of new systems such as mobile intercontinental ballistic missiles, hypersonic glide vehicles, quieter submarines and air refueling capabilities.

These have increased the PLA’s ability to project



power beyond a range needed for defense. Much of Beijing’s weapons development is designed to prevent the U.S. military from deploying into the Western Pacific in a crisis, and PRC leaders often speak of a strategy designed to deny access to the theater. “If their words are to be believed, cyber and long-range precision strikes on key locations in the United States will be part of this strategy,” the generals’ paper states.

Although Russia has long possessed the capability to strike North American targets while remaining below the nuclear threshold, the Kremlin more recently has dedicated significant resources toward creating a long-range precision conventional strike capability. By deploying stealth air- and sea-launched cruise missiles and modernizing the aircraft and submarines that deliver them, Russia has gained its first conventional capability to strike the continental U.S.

With stakes so high, NORAD continues to innovate, train and strategize to meet the challenge. After NORAD aircraft intercepted six Russian Tu-142 maritime patrol aircraft in the Alaskan ADIZ in late August 2020, VanHerck noted the surge in Russian activity near North American coastlines. “This year, we’ve conducted more than a dozen intercepts, the most in recent years,” he said. “The importance of our continued efforts to project air defense operations in and through the North has never been more apparent.”

ARCTIC DETERRENCE

Denmark May Use Stealth F-35s Over Greenland

THE WATCH STAFF

Danish military officials say the U.S.-made F-35 fighter jet is poised to play a key role in Denmark's air defense and could be used in Greenland as the abundant natural resources of the Arctic lure great power competitors to the region.

Maj. Gen. Anders Rex, commander of Air Command Denmark for the Royal Danish Air Force, told Defense News in August 2020 that some of the 27 F-35s that Denmark purchased from the United States will be outfitted with a drag chute that will enable them to land on icy runways. "Coupled with the Greenlandic decision to extend a number of air fields to more than 2,000 meters, it gives vastly increased operational opportunities for fighter operations," Rex wrote, adding that the F-35's data-collection and data-sharing capabilities can enhance pilots' situational awareness.

"Air power is of vital importance in the Arctic, given the core air power characteristics, but it must be in a joint and combined framework, enabling future multidomain and network-based operations in the Arctic region," Rex wrote. "The Royal Danish Air Force will work toward that objective."

He emphasized that no decision had been made about whether the F-35s will carry out missions over the Arctic, but his announcement came as Danish officials were showing increased interest in cooperating with Greenlandic authorities on defense. Greenland, the world's largest island, is a self-governing part of Denmark.

As the U.S., the People's Republic of China and Russia show renewed interest in Arctic military and economic activities, Denmark has been strengthening its defense and security policy efforts in the region.

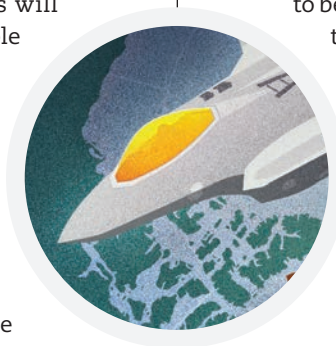
"We have seen a new security policy dynamic gain ground in the Arctic in recent years," the Danish Ministry of Foreign Affairs wrote to the *High North News* newspaper in August 2020. "There is increased interest in the region from many sides. It is thus decisive for the Danish Realm to be proactive in this new situation. We will secure the necessary presence in the Arctic in light of this development, and create a better situational awareness in the region."

The ministry recently sent a political advisor to Greenland's capital, Nuuk, to establish closer security ties. In June 2020, the U.S. reopened its consulate in Nuuk, which had been closed since 1953.

Denmark's decision to send an envoy to Greenland is part of a series of Arctic initiatives, the *High North News* reported. In August 2020, the

Danish Armed Forces established an office in Nuuk, and the military announced that it wants to reestablish a military radar station on Denmark's Faroe Islands, a North Atlantic archipelago about 320 kilometers northwest of Scotland.

"We are talking about extra eyes and ears in the Arctic and the North Atlantic in the form of various forms of surveillance," the Foreign Affairs Ministry told the *High North News*. "Beyond contributing to peace and security, these capacities may also be used for civilian purposes







An F-35 demonstration team pilot performs a high-speed pass during the Arctic Lightning Airshow at Eielson Air Force Base in Alaska.

SENIOR AIRMAN ALEXANDER COOK/
U.S. AIR FORCE

Greenland, the world's largest island, lies between the Arctic and Atlantic oceans. It is an autonomous territory of Denmark. Although adjacent to North America, Greenland has been politically and culturally associated with European colonial powers, specifically Denmark and Norway, for more than a millennium.





The Greenland ice cap has been retreating in recent years, leading to increased shipping because the waters are more navigable.

THE ASSOCIATED PRESS

“With additional budgetary and policy attention to increasing readiness, European allies have the opportunity to significantly enhance combat air power over the coming decade,”

~ October 2020 Rand Corp. report

such as for instance environmental monitoring and contributions in search and rescue.”

As for the addition of F-35 stealth fighters to the region, the NATO alliance is quickly gaining an edge over Russia in the event of a high-intensity conflict, according to an October 2020 Rand Corp. report. The report said Russian military and political leaders are concerned about NATO’s air power advantage as European countries purchase the fifth-generation fighter jet.

Seven European NATO nations — Belgium, Denmark, Italy, the Netherlands, Norway, Poland and the United Kingdom — either operate or plan to buy F-35s. The countries by 2025 will collectively own more than 200 of the aircraft.

The Rand report concluded that the growing number of stealth aircraft in Europe represents a trend in the right direction. “With additional budgetary and policy attention to increasing readiness, European allies have the opportunity to significantly enhance combat air power over the coming decade,” the report stated.

European allies soon will have more fifth-generation F-35s stationed in the region than the U.S. has in the theater. By 2030, they will have about 400 F-35s. And

while protecting NATO allies is paramount for the U.S., the Arctic region also represents a strategic area for homeland defense.

In a January 2019 article for Defense News, then-U.S. Air Force Chief of Staff Gen. David Goldfein and then-Secretary of the Air Force Heather Wilson wrote that the Arctic represents a northern approach to the U.S. and that its “geo-strategic significance is difficult to overstate.”

“Key defense assets dot the landscape. ... One way to view the region’s growing importance: By 2022, Alaska will be home to more advanced fighter jets than any place on Earth,” the article stated.

Arctic partners of the U.S. are welcoming its engagement. The Danish Foreign Ministry told the *High North News* that increased U.S. involvement in the Arctic and North Atlantic, including Greenland, is a “positive thing.”

“Greenland is geographically located close to the USA, and increased cooperation and economic ties between the USA and Greenland can thus only be seen as natural,” the ministry stated. “The USA is our closest partner outside of Europe, and the USA along with NATO guarantees our security.” ☐

SHARING KNOWLEDGE

The Watch is a magazine provided free to those responsible for homeland defense.

CONTRIBUTE TO *THE WATCH*

Send all story ideas, letters to the editor, photos, opinion articles and other content to *The Watch's* editorial staff at n-nc.peterson.n-ncj3.mbx.the-watch@mail.mil

SUBMISSION TIPS

- Articles should not exceed 1,500 words.
- Please include a short biography and contact information with each submission.
- Photo file size should be at least 1 megabyte.

RIGHTS

Authors retain all rights to their original material. However, we reserve the right to edit articles to meet length and style requirements. Article submission does not guarantee publication. By contributing to *The Watch*, you agree to these terms.

FOR A
FREE
SUBSCRIPTION:

Email us at:
n-nc.peterson.n-ncj3.mbx.the-watch@mail.mil

Or write to: *The Watch*
Program Manager
HQ USNORTHCOM
250 Vandenberg St., Suite B016
Peterson AFB, CO 80914-38170

Please include your name, occupation, title or rank, mailing address and email address.

THE WATCH

VIEW US ONLINE: THEWATCH-MAGAZINE.COM

For more on security and defense issues around the globe, visit the links below:

UNIPATH-MAGAZINE.COM | IPDEFENSEFORUM.COM | ADF-MAGAZINE.COM | PERCONCORDIAM.COM | DIALOGO-AMERICAS.COM