THE WATCH

v1

I ARCTIC DEFENSE
NATIONS ALIGN TO PROTECT RESOURCES

II BULL'S-EYE
MISSILE INTERCEPT LIFTS PROGRAM

III EYES ON THE SEAS
NORAD'S MARITIME MISSION

CONTENTS

THE WATCH // **HOMELAND DEFENSE**

> “There is no mission more sacred than defending the homeland.”

U.S. AIR FORCE GEN. TERRENCE J. O’SHAUGHNESSY,
COMMANDER OF U.S. NORTHERN COMMAND

v1

Features

DEPARTMENTS

ABOUT THE COVER

This illustration by *The Watch* staff represents the motto of U.S. Northern Command: "We Have the Watch."

Dear Readers,

Welcome to the first edition of *The Watch*, a magazine published by U.S. Northern Command focusing on homeland defense. This inaugural issue explores the changing threat environment — from troubling advances in adversaries' missile capabilities to new vulnerabilities in the cyber sphere — and how partners are working together more than ever to safeguard their homelands.

Defense strategies must evolve as the physical nature of the planet evolves. The Arctic region, for example — once a nearly impenetrable plug of ice and hazardous weather — becomes increasingly more accessible as ice caps recede. The melting ice exposes deposits of oil, gas and minerals to extraction, opens shipping lanes, draws countries into competition and spurs the militarization of a once-overlooked region.

Such evolving defense challenges often are met by partners working together. Norway, for example, decided in January 2017 to allow U.S. Marines to deploy inside its borders — a first since Norway joined the North Atlantic Treaty Organization (NATO) in 1949. While the countries train together to conduct cold-weather operations, they also demonstrate the strength of the NATO alliance. Norway and its neighbors have spent the past year reasserting their commitment to the alliance and increasing defense spending in the face of Russian aggression in Crimea and eastern Ukraine.

When it comes to 21st-century warfighting, however, not every battle is fought with tanks, airplanes and ships. Some battles are won in space, while others are waged on the internet. In this edition, we'll explore a U.S. Pentagon program that involves cutting-edge technology. Innovative ground defenses destroyed a mock intercontinental ballistic missile in space and never allowed it to enter the atmosphere or threaten the U.S. homeland.

By establishing strong alliances and staying abreast of disruptive technology, the United States and its partners and allies collectively defend their homelands every day. We hope you find this edition of *The Watch* insightful and informative.

Regards,

THE WATCH STAFF

THE WATCH

Homeland Defense

Volume 1 2018

USNORTHCOM LEADERSHIP

TERRENCE J. O'SHAUGHNESSY
General, USAF
Commander

REYNOLD N. HOOVER
Lieutenant General, USA
Deputy Commander

RICHARD J. GALLANT
Major General, USA
Chief of Staff

CONTACT US

THE WATCH

The Watch
Program Manager,
HQ USNORTHCOM
250 Vandenberg St. Suite B016
Peterson AFB, CO 80914-3817O
email:
n-nc.thewatch@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)

U.S. Air Force F-22 Raptors fly over the Arc de Triomphe during the Bastille Day military parade on the Champs-Elysees in Paris, France, in July 2017.

REUTERS

LITTLE TECHNOLOGY, BIG IMPLICATIONS

How small satellites are revolutionizing space

ERICA SULLIVAN, LOS ALAMOS NATIONAL LABORATORY

On a clear morning in Sriharikota, India, in mid-February 2017, a rocket launched carrying a record-breaking 104 satellites, including 101 CubeSats.

CubeSats are nothing new. A type of small satellite comprising units measuring 10 centimeters by 10 centimeters by 10 centimeters, they were first developed at Cal Poly and Stanford universities in the late 1990s as a training tool for aerospace engineering students. ("SmallSats" are lighter than 500 kilograms; so all CubeSats are SmallSats, but not all SmallSats are CubeSats.) It wasn't long before governments began to look for ways to use CubeSats and other small satellites to bolster national security.

It's no coincidence that the rise in interest in these smaller-than-a-dorm-refrigerator satellites coincided with the awareness that existing satellites were vulnerable. In 2007, China proved this when it used a missile to obliterate one of its own satellites. Then there's the threat of cyber attack. The recent ransomware virus that infected hundreds of thousands of computer systems around the globe and shut down hospitals and train stations was a stark reminder of the power of hackers. If that cyber attack was so debilitating on Earth-based systems, imagine what a carefully orchestrated cyber attack on a space-based asset would do. The results could be catastrophic.

Virtually every military mission relies, to some extent, on satellites. Communications satellites not only provide reliable communications for command, they control land, sea and air forces as well. Meteorological satellites provide up-to-date weather information to field units in every branch of the military. Navigation satellites provide accurate positioning — within a few meters — for troops, planes and ships. Space-based surveillance systems provide treaty-monitoring capability during peacetime and serve as essential warning systems during conflict.

For the civilian arm of the government, satellite imagery is indispensable for disaster planning and response, mapping, urban planning and traffic monitoring. Then there are commercial uses: satellite phones, the internet, television, navigation and commercial tracking, resource exploitation — even predicting the weather for air travel or planting crops.

A successful attack on just one of those satellites could have far-reaching negative consequences for homeland defense and the economy.

TECHNOLOGICAL ADVANTAGES

What if, instead of one giant satellite providing critical national security functions, there were a hundred small satellites doing the same thing? The target would not only be smaller, but it would be dispersed — making a cyber criminal's job significantly more difficult.

Small satellites boast a lot of positives. First and foremost, they're inexpensive. The average large satellite can cost anywhere from U.S. $500 million to U.S. $1 billion or more to build and launch. That's a hefty price for any budget. Small satellites, by comparison, are a bargain.

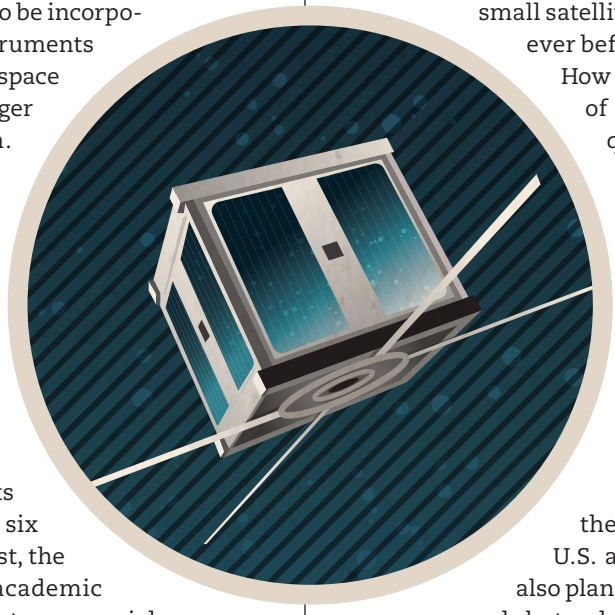
For example, Los Alamos National Laboratory has built and launched a set of CubeSats into low-Earth orbit (LEO) for a U.S. Department of Defense sponsor at a cost of about U.S. $150,000 per satellite. Also, the less expensive hardware means more technology can be acquired — enabling greater geographic coverage for observation and detection missions such as Earth/wave movement,

An H-IIA rocket, carrying a Michibiki 2 satellite, lifts off from Tanegashima Space Center in Japan. REUTERS

seismic and volcanic activity detection, and atmospheric measurements.

Furthermore, by using less expensive platforms such as CubeSats and SmallSats, space scientists could test advanced concepts such as reconfigurable computing in space. In the past, once a satellite was in orbit, operators could do little to alter it. It would operate according to its original programming. Not so with CubeSats, which space scientists have made reprogrammable to allow for mission changes and improvements.

It also allows for a more agile approach to space hardware. Constrained mission needs enable rapid, focused development. While a large satellite can take a decade to design and build, space scientists can do the same with a CubeSat in a year or less. These satellites also enable more testing in the operational environment rather than in simulated environments on the ground, and they allow cutting-edge technologies to be incorporated as they hit the market. Instruments and components can be tested in space before they're integrated into larger platforms for the final mission. These demonstration and validation missions greatly inform the design of instruments for any size satellite.



REVOLUTIONIZING ENGINEERING

For these reasons, small satellites revolutionize how scientists engineer space systems. A staggering 2,400 SmallSats and CubeSats will be launched during the next six years, experts estimate. In the past, the commercial, government and academic sectors used SmallSats equally, but commercial use is expected to leapfrog the rest soon. Over the next three years, commercial use of small satellites is anticipated to account for more than 70 percent of launches.

Small satellites get to LEO at a lower cost and subject the satellite to fewer radiation effects. Also, LEO allows the satellite to be closer to targets, improving the resolution of imagery, enabling lower-power communications and decreasing communications lags.

Increasingly, the government, industry and academia are looking for ways to use small satellites in orbits beyond LEO. For example, at Los Alamos, scientists and engineers would like to use small satellites and CubeSats for deep space and interplanetary exploration missions. For these technically challenging missions, smaller, less expensive satellites create the opportunity to spread technical risk over redundant systems and to collect data from more locations.

MANAGING RISK, FOSTERING COOPERATION

A leading challenge is to develop faster and smarter than the rest. The U.S. and its allies and partners must acknowledge that many nations now have access to space, and it must become a strategic military priority to introduce resiliency and redundancy into space systems. In short, nations must spread the risk. The good news is that advances in distributed computing and machine learning mean scientists can create a distributed network that can heal itself. So, if one satellite out of a constellation of a hundred is damaged, the others can compensate.

Also, the technology must be optimized. If more small satellites are gathering more data than ever before, the next question becomes: How will that data be processed? Then of course, there are myriad other questions as well: How do nations secure their networks? How do nations make their satellites impervious to space weather? Los Alamos, for one, is leveraging decades of experience developing space instruments, understanding of the extreme space environment and supercomputing prowess to answer these questions.

It's not only about developing the right technology, however. The U.S. and its allies and partners must also plan carefully — not just on a national scale but a global one. Just as the international community has jointly designated international shipping and air traffic routes, the international community needs to collaborate to figure out how to work cooperatively to regulate space.

The reality is, during the next few decades, space will become more and more crowded, and how it's used will change the world. That change is coming quickly. Will the international community rise to meet these challenges before they overwhelm us? If the answer is yes, nations must start working together to solve these issues now.

Erica Sullivan is the program manager of Agile Space at Los Alamos National Laboratory.

ARCTIC PARTNERS

Deployment to Norway fortifies NATO alliance

THE WATCH STAFF

When more than 300 U.S. Marines arrived on the snowy slopes of central Norway in January 2017, it marked the first time since NATO was founded in 1949 that foreign troops have been stationed in the Arctic country. The North Atlantic Treaty Organization (NATO) allies announced that cold-weather training was their priority, although Norway's decision to invite U.S. troops to stay for up to a year on a rotational basis comes while many Nordic countries are fortifying homeland defenses because of Russia's actions near their borders.

Norway joined NATO in 1949 on the condition that no foreign combat troops be permanently stationed on its territory during peacetime. The reversal is an "intentional policy change and one that follows the Norwegian government's request for the strengthening of NATO's military presence in the High North," Henrik Urdal, director of the Peace Research Institute Oslo, told *The Watch*. "It is a response to the changing European security climate and specifically to increased Russian military presence in a region that is a top Norwegian foreign policy priority."

Norwegian officials said the deployment demonstrates a strengthening of the NATO partnership. "The U.S. initiative to augment their training and exercises in Norway by locating a Marine Corps Rotational Force in Norway is highly welcome and will have positive implication for our already strong bilateral relationship," then-Norwegian Minister of Defence Ine Eriksen Søreide said in a prepared statement.

Søreide has been rallying NATO members and Norway's neighbors to bolster their homeland defenses since Russia's annexation of Crimea and its military interference in eastern Ukraine in 2014. "Norway is NATO in the North, and we share a border with an increasingly assertive neighbor with superpower aspirations," Søreide told a security conference in Oslo, Norway, in February 2017. Russia has "modernized its Armed Forces, significantly increased its military presence in the High North, reintroduced the old East versus West schismatic thinking, engaged in subversive actions against Western democracies, violated international law and undermined European stability," she added.

Russia's military activities in the region extend beyond Crimea and Ukraine.

Over the previous two years, NATO commanders reported seeing more Russian submarines in the North Atlantic than they have seen since the end of the Cold War. NATO also recorded a sharp increase in Quick Reaction Alert scrambles to encounter Russian military planes in the Baltic and Black Sea regions. NATO's European forces scrambled aircraft 480 times in 2014, and 400 of those involved Russian military aircraft. In 2016, that number soared to 807, and the majority — 780 — were responses to Russian military aircraft, a Jane's 360 report noted.

"The U.S. initiative to augment their training and exercises in Norway by locating a Marine Corps Rotational Force in Norway is highly welcome and will have positive implication for our already strong bilateral relationship."

Ine Eriksen Søreide, then Norwegian minister of defence

U.S. Marine Cpl. Anthony Sixtos, a rifleman with the rotational force in Europe, fires an AT-4 rocket at a live-fire range in Leksdal, Norway.
CPL. VICTORIA ROSS/
U.S. MARINE CORPS

U.S. Marines walk through the tunnels of Hegra fortress near Stjørdal, Norway. The fortress was built in 1910 to defend against a Swedish invasion and is famous for resisting an attack by Nazi Germany in 1940.
CPL. EMILY DORUMSGAARD/
U.S. MARINE CORPS

While the U.S. presence in Norway is small, it sends a symbolic message about NATO determination, Urdal said. "The security guarantee provided by NATO and the U.S. forms the cornerstone of the Norwegian security policy," Urdal said. "While the deployment of 300-plus U.S. Marines has little impact on Norway's military capabilities, it signals resolve on the part of the alliance to uphold a strong presence in the region."

Norway's neighbors are also showing increased resolve.

- Finland announced in February 2017 that it will increase annual defense spending by U.S. $178 million and boost troop totals by about 20 percent to 280,000. It also stepped up military cooperation with neighboring Sweden following Russia's annexation of Crimea in 2014.
- A month after Finland's announcement, Swedish Minister of Defence Peter Hultqvist announced that his country would reintroduce military conscription for men and women in 2018 and boost defense spending by U.S. $55 million for the year.
- NATO member Denmark in January 2017 said it, too, plans to increase military spending in response to Russian missile deployments in the Baltics.

UNDERGROUND WEAPONS CACHE

The U.S. Marines who arrived in Vaernes, Norway, are part of a newly created Marine Rotational Force-Europe. The unit, which served a six-month rotational deployment, is working with the Norwegian Ministry of Defence to improve the Marines' ability to fight in extreme cold. Lt. Gen. John Wissler, then comander of the Marine Corps Forces Command, exhorted Marines to pass on what they learned from their cold-weather training, military.com reported. "As a Marine Corps, we've been very used to operating in sort of jungle and desert environments, but we're not as good at operating in Arctic environments as we need to be," he said in May 2017. "This company of Marines, and those Marines that accompanied you in your training, are capable of engaging and locating, closing with and destroying by fire and maneuver any enemy that we would encounter in an Arctic environment."

The allies use underground caves in Norway to preposition gear to speed deployments. U.S. Marines and Norwegian Soldiers store battle tanks, artillery and logistics equipment in the caves. "We have prepositioned gear, both in caves and on ships, and it allows forces from the United States to come on out and fall in on gear that is already forward-deployed versus bringing all that gear with us," said Col. William Bentley, then operations officer for the 2nd Marine Expeditionary Brigade, according to a report on the U.S. Marine Corps website.

The gear has supported missions all over the world, including the 2003 invasion of Iraq, the ongoing fight against the Islamic State in Iraq and Syria and delivery of humanitarian assistance to Turkey after the 2011 earthquakes.

Lt. Gen. John Wissler, center, then commander of U.S. Marine Corps Forces Command, speaks with Marines in Norway while looking over an assembly area where equipment is prepositioned.

CPL. EMILY DORUMSGAARD/ U.S. MARINE CORPS

U.S. Marines conduct live-fire drills during exercise Ymir Viking in Rena, Norway. Ymir Viking is a monthlong training exercise that tests the capabilities of Marines to operate in cold weather.

CPL. CAREAF HENSON/ U.S. MARINE CORPS

TAKING STOCK OF SEA DEFENSES

While the underground caves support ground operations, NATO has taken a harder look at its maritime defenses, too, as Russia upgrades its Northern Fleet off Norway's coast. "Russia is expanding its undersea operations as part of a broader strategy of coercion aimed at its neighbors, the North Atlantic Treaty Organization and the United States," said a July 2016 report from authors Kathleen Hicks, Andrew Metrick, Lisa Sawyer Samp and Kathleen Weinberger at the Center for Strategic and International Studies (CSIS), a Washington, D.C.-based think tank.

The report, titled "Undersea Warfare in Northern Europe," cited a number of Russian provocations, including probable territorial violations of Swedish and Finnish waters by Russian submarines and Russian submarine activity near the United Kingdom's submarine base at Faslane, Scotland.

It also pointed out a highly publicized 2014 incident when the Swedish Navy spent a week searching the Stockholm archipelago with helicopters and minesweepers after what was believed to be the spotting of a Russian submarine in Swedish waters. After a similar sighting, the Finnish Navy dropped depth charges into the water to warn off intruders in April 2015.

While Norway and U.S. ground forces continue to collaborate, the allies should also build organizational structures through the NATO-Nordic Defense Cooperation to establish an anti-submarine warfare center of excellence in the region, the CSIS report said. It also recommended that NATO reopen the Keflavik Naval Air Station in Iceland and that Norway reactivate its Olavsvern submarine support facility.

The Olavsvern base is "ideal for supporting submarine operations in the extreme North Atlantic and Arctic seas," the report said. It is strategically located at the confluence of the Barents Sea and the extreme North Atlantic. During the Cold War, NATO submarines used it as a resupply hub. The base was closed in 2009. If Norway reopens a portion of the facility, it could support a rotational presence of British, French, Norwegian and U.S. submarines, the report said.

FILLING THE GAPS

Norway has no current conflict with Russia. The countries cooperate on coast guard operations, search-and-rescue operations and on guarding their mutual border.

Norway and its neighbors have watched, however, as Russia developed a sophisticated submarine fleet and tested high-precision, long-range missiles in the North Atlantic. The need for readiness, Norwegian commanders say, is paramount.

"We are not in a conflict with Russia, and we have never had a border dispute with them in 1,000 years, but after Ukraine we changed our posture," Lt. Gen. Rune Jakobsen, commander of the Norwegian Joint Headquarters, told *The Guardian* newspaper. "They are developing new capabilities, especially submarines, very fast. If we leave a vacuum, they will fill it."

VACCINE PROGRESS STALLS

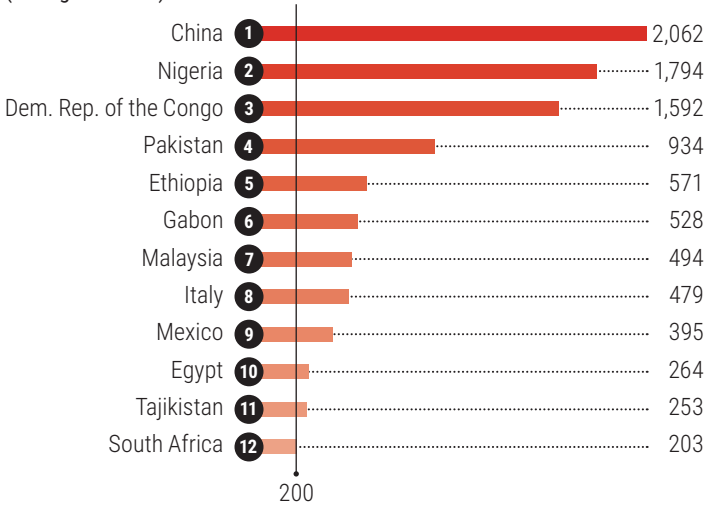
New estimates from the World Health Organization (WHO) and UNICEF have found that **12.9 million infants, or nearly 1 in 10 around the world, didn't receive any vaccinations in 2016.** Consequently, these infants missed the first dose of the combined vaccine against **diphtheria-tetanus-pertussis (DTP3)** and the vaccine to prevent **measles, mumps and rubella (MMR).**

PREVENTABLE DISEASES

- **Measles, mumps and rubella** are all viral infections. Measles can cause a rash, cough, runny nose, eye irritation and fever. It can lead to ear infection, pneumonia, seizures, brain damage and death. Of these diseases, measles is the one still common in many parts of the world.
- **Diphtheria** is a bacterial infection that can cause breathing difficulties and death.
- **Tetanus** germs grow in puncture wounds caused by dirty nails, tools, splinters and animal bites.
- **Pertussis**, also called whooping cough, is a disease of the respiratory tract caused by bacteria in the mouth, nose and throat.

Countries With Over 200 Cases of Measles in 2017

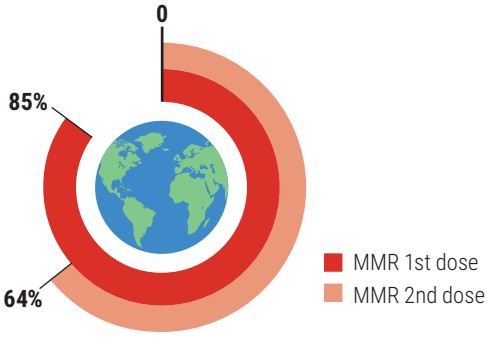
(through March 9)



STRIDES TOWARD FULL COVERAGE

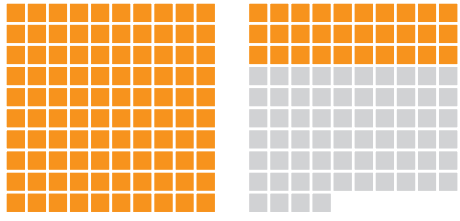
MMR

About **85 percent** of children have been vaccinated with the first dose of measles vaccine by their first birthday through routine health services, and **64 percent** with a second dose. WHO says these coverage levels remain short of those required to prevent outbreaks.



DTP3

New statistics show that **130 of the 194** World Health Organization member states reached the WHO goal of at least **90 percent** coverage for DTP3.



Health officials vaccinate children for measles, mumps and rubella in Yemen, left, and south Wales, right.

REUTERS

CHALLENGES REMAIN

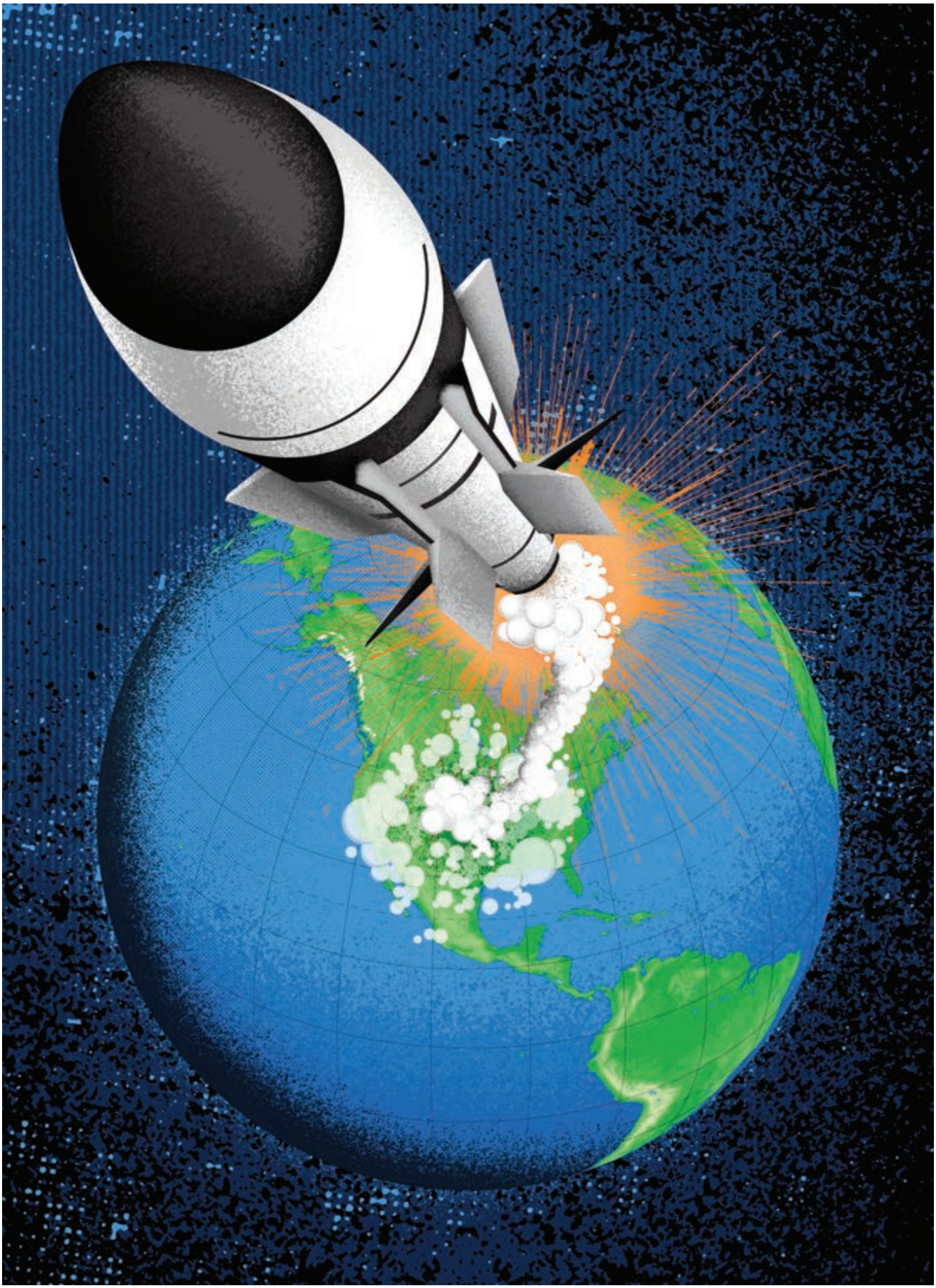
MMR

Globally, **more than 50 percent** of the 20.8 million children who did not receive a dose of measles vaccine in 2016 came from only six countries — Ethiopia, the Democratic Republic of the Congo, India, Indonesia, Nigeria and Pakistan.

DTP3

Eight countries had **less than 50 percent** coverage, including the Central African Republic, Chad, Equatorial Guinea, Nigeria, Somalia, South Sudan, Syria and Ukraine.

Source: World Health Organization, UNICEF

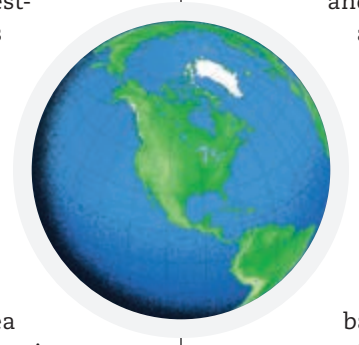


IGNITING OPTIMISM

Long-range missile defense system reaches new high

THE WATCH STAFF

The Pentagon's successful test of its ground-based midcourse defense (GMD) anti-missile system on May 30, 2017, could not have come at a more opportune time. Despite global condemnation, North Korea had been accelerating its long-range intercontinental ballistic missile (ICBM) testing with the stated goal of building a nuclear-tipped weapon capable of striking the United States. Recent test-firings have demonstrated North Korea's ability to attain its goal sooner than many experts had believed, adding a renewed urgency to developing an effective GMD system.



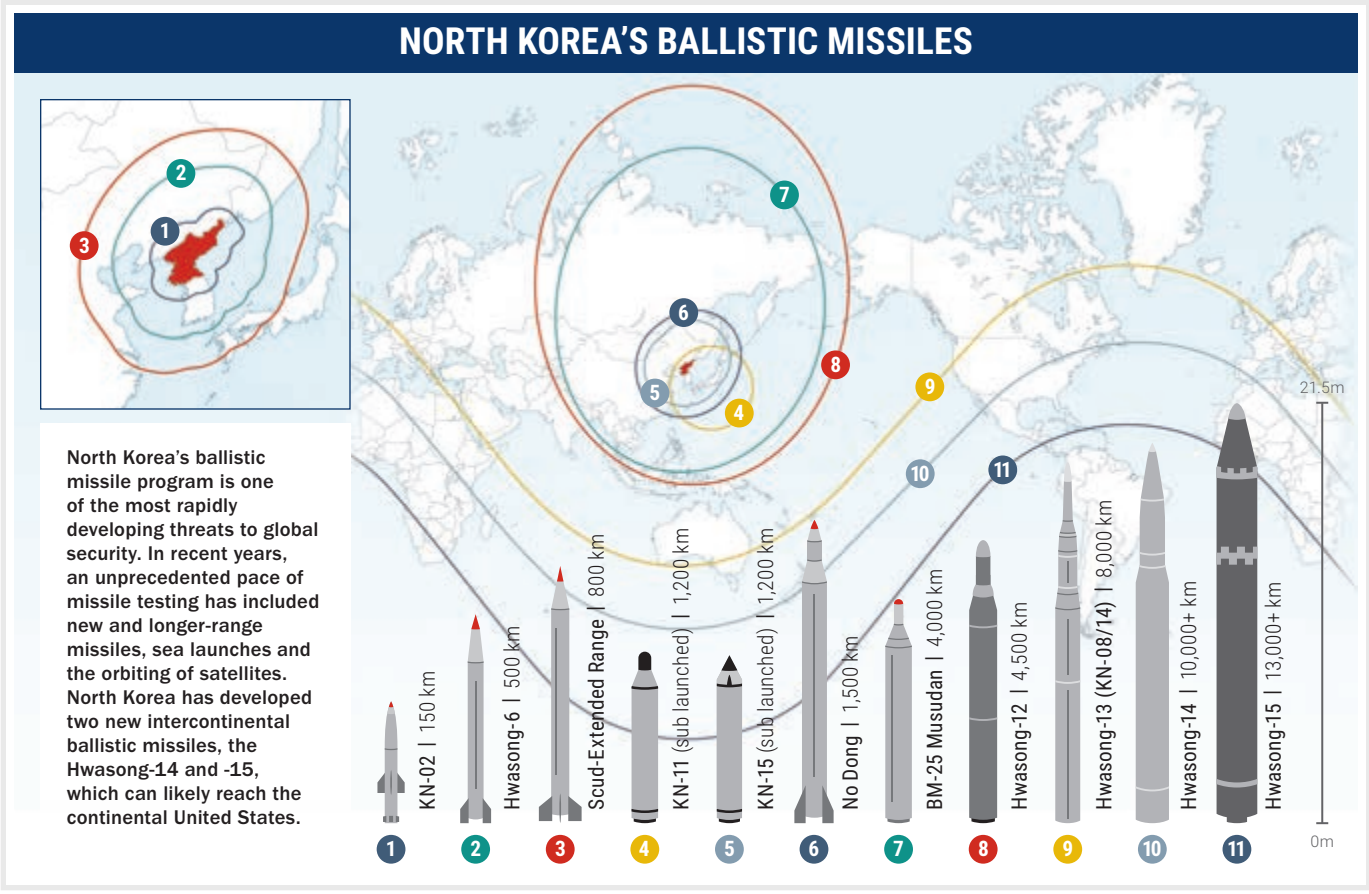
The missile defense system is part of an array of efforts by the U.S., its allies and partners to deter North Korea from developing nuclear weapons and defend against them. North Korea agreed in the historic June 12, 2018, summit with U.S. President Donald Trump to halt tests and work toward denuclearizing the Korean Peninsula, although experts agree that could take many years to achieve.

The successful test used a sea-based radar system in the Pacific Ocean to track a mock ICBM and feed data into the GMD system. A "kill vehicle" equipped with tracking sensors separated from its missile and, moving at speeds exceeding 6.4 kilometers per second, destroyed the target in space by moving directly into its path. "The intercept of a complex, threat-representative ICBM target is an incredible accomplishment for the GMD system and a critical milestone for this program," Vice Adm. James D. Syring, director of the U.S. Missile Defense Agency (MDA), said in a prepared statement. "This system is vitally important to the defense of our homeland, and this test demonstrates that we have a capable, credible deterrent against a very real threat."

THE CHALLENGE

The path to that successful test can be traced to the 1999 National Missile Defense Act, which directed the Pentagon to create a system capable of protecting the U.S. from a long-range ballistic missile attack. Three years later, President George W. Bush called for a workable missile defense system to be in place by 2004. In response, the newly formed MDA developed a land-based missile system to track and intercept ICBMs in space, before descent into the atmosphere.

Using land, sea and space radars, the system detects a threat and triggers the launch of a three-stage booster rocket with an interceptor missile. Atop the interceptor is a detachable exoatmospheric kill



Source: Center for Strategic and International Studies | https://missilethreat.csis.org/country/dprk/

> "If left on his current trajectory, [North Korean leader Kim Jong Un] will ultimately succeed in fielding a nuclear-armed missile capable of threatening the United States homeland."
>
> Lt. Gen. Vincent R. Stewart, director of the U.S. Defense Intelligence Agency

vehicle (EKV) with onboard sensors and thrusters that set a trajectory for colliding with an incoming warhead. The collision is described as the equivalent of hitting a bullet with a bullet. Fallout from the destroyed ICBM occurs in space, sparing the targeted populations below. The GMD's long-range targets differentiate the system from the Pentagon's existing Aegis, Patriot and Terminal High Altitude Area Defense (THAAD) systems, which are designed to respond to medium- and short-range threats.

The MDA housed its interceptor missiles at two sites: a repurposed World War II-era military base in Fort Greely, Alaska, and at Vandenberg Air Force Base in California. Initial testing results showed improvement over several years, including a June 2014 test during which the GMD system destroyed a test target moving in space over the Pacific Ocean.

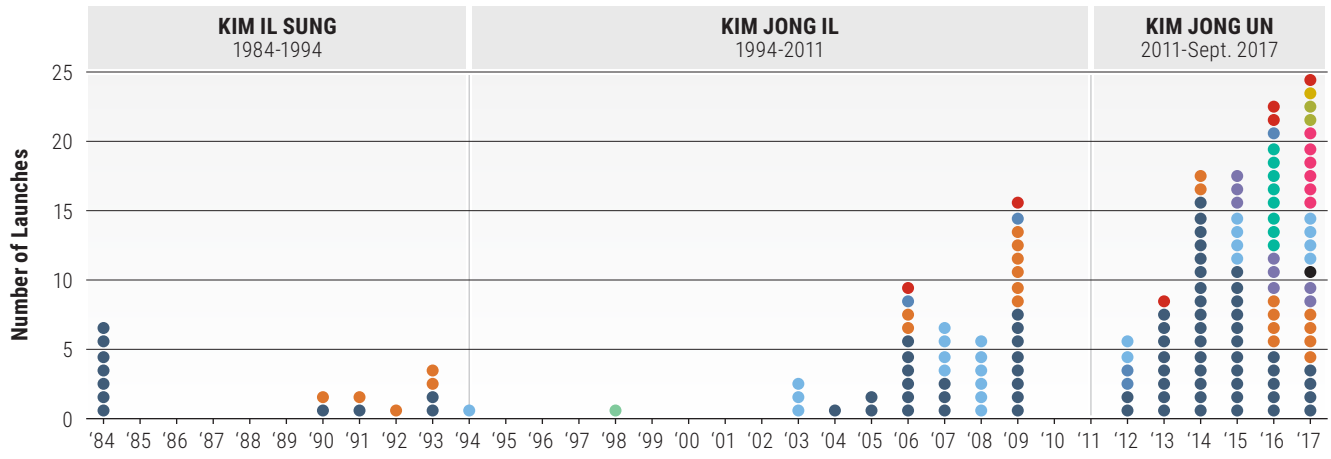
MAY 30, 2017

Then on May 30, 2017, the intercept of a mock ICBM exceeded all previous tests. The MDA launched an unarmed ICBM from Kwajalein Atoll, prompting the launch of an intercept missile from Vandenberg AFB. Radar in the Pacific Ocean tracked the missile while sensors on an EKV with newly redesigned guidance thrusters calculated the speed and direction needed to intercept the target. The direct collision represented the first successful live-fire GMD test against an ICBM-class target.

The results ignited greater optimism in a program that is seeking nearly U.S. $1 billion for missile defense in 2018, when it expects to have 44 ground-based interceptors in place at Fort Greely and Vandenberg AFB, the most ever in the program's history. In development is a redesigned EKV that could destroy multiple targets in a single launch, and improved interceptors and sensors. The complexity of the task and the system's testing history continue to raise concerns

An intercontinental ballistic missile is test-fired in this undated picture provided by the North Korean news agency in Pyongyang. REUTERS

NORTH KOREAN MISSILE LAUNCHES

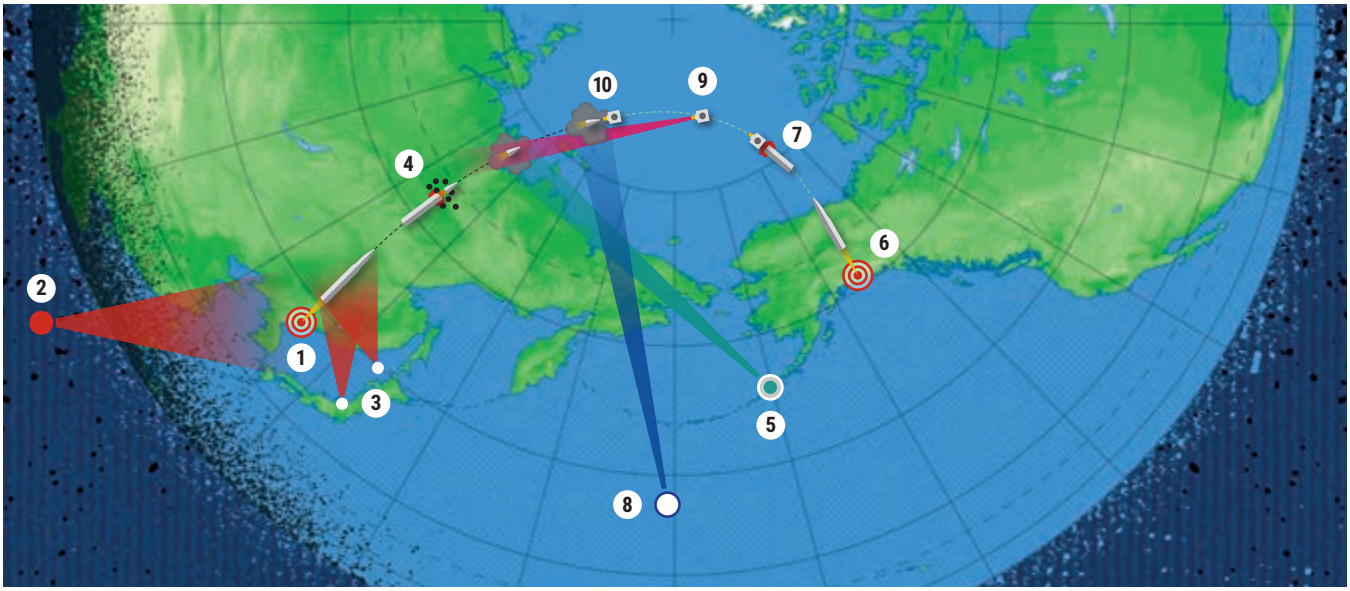


- Hwasong-15 (13,000 km)
- Hwasong-14 (10,000 km+)
- Hwasong-12 (4,500 km)
- BM-25 Musudan (2,500-4,000 km)
- Cruise Missile (KH-35, KN-01, 150-260 km)
- KN-11 SLBM (Sub-launched ballistic missile) / KN-15 (900-2,000 km)
- MRBM (Medium-range ballistic missile) (Scud-ER, No Dong, 1,000-1,500 km)
- Nuclear Test
- SRBM (Short-range ballistic missile) (Scud variants, KN-02, 150-1,000 km)
- Taepodong-1 (2,000-5,000 km)
- Taepodong-2 / Unha-3 (4,000-15,000 km)
- Unknown

Accounts for full flight tests only. Does not include partial tests of missile subsystems such as static engine firings or cold-launch ejection tests, tests of air-defense systems, or short-range rockets and artillery firings.

Source: Center for Strategic and International Studies | https://missilethreat.csis.org/country/dprk

INTERCEPT SEQUENCE



1. Threat missile launch
2. Infrared satellites detect launch
3. Forward-based radars track missile
4. Missile releases warhead and decoys (threat cloud)
5. Ground-based radar tracks threat cloud
6. Ground-based interceptor launch
7. Exoatmospheric kill vehicle (EKV) separates from interceptor
8. Sea-based X-band radar tracks threat cloud, attempts discrimination
9. EKV views threat cloud
10. Intercept

Source: Center for Strategic and International Studies | https://missilethreat.csis.org/system/gmd

among critics. But the success in May 2017 prompted the Pentagon's Operational Test and Evaluation office to upgrade its GMD assessment to "demonstrated capability to defend the U.S. homeland from a small number of intermediate-range or intercontinental missile threats with simple countermeasures."

RAISING ALARMS

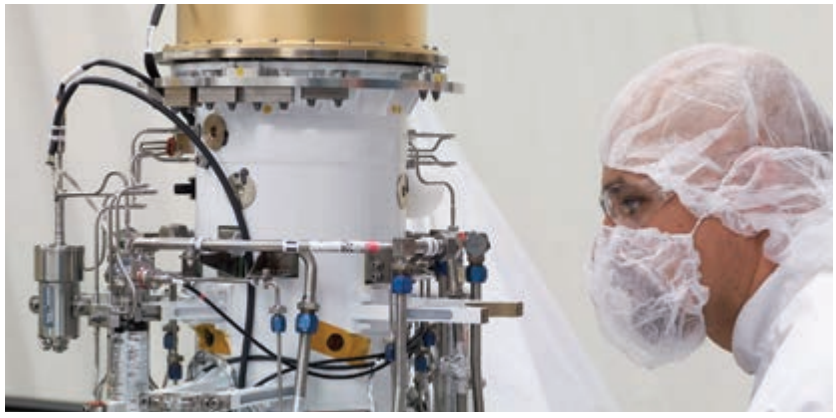
Just weeks after that successful test, North Korea raised the stakes for the U.S. to build and maintain a reliable GMD system. Twice in July 2017 the North Koreans test-fired ICBMs capable of reaching most of the U.S. Several more launches followed before the end of 2017. Based on government assessments, North Korea now possesses the technology to shrink a nuclear weapon to fit atop an ICBM, though it remains uncertain whether that nuclear weapon could withstand re-entry into the atmosphere. Either way, the tests eliminated any doubts about North Korea's ability to launch ICBMs that can reach the continental U.S.

It's a goal North Korea has been building toward at an accelerated pace. In 2009 it test-fired a missile in violation of the 1953 Korean cease-fire. Over the past five years, it has flouted United Nations Security Council resolutions by detonating underground nuclear devices and conducting dozens of missile tests, each one raising new alarms. For instance, past missiles were powered by liquid fuels that took hours to load, leaving them exposed to surveillance. Solid fuels now being used allow the North Koreans to move a missile from a secure position and launch within minutes, leaving little time for targeted countries to prepare. Within 10 years North Korea could wield a nuclear arsenal with ICBMs capable of being launched from land, air and sea, some analysts believe. "If left on his current trajectory, [North Korean leader Kim Jong Un] will ultimately succeed in fielding a nuclear-armed missile capable of threatening the United States homeland," said Lt. Gen. Vincent R. Stewart, director of the U.S. Defense Intelligence Agency.

PROLIFERATION

North Korea isn't the only country with a global missile system that poses a threat to the U.S. or its interests abroad. Iran's desire to have a strategic counter to the United States could drive it to field an ICBM. Progress in Iran's space program could shorten the pathway to an ICBM because space launch vehicles use inherently similar technologies. Russia has an array of ICBMs and cruise missiles, and China is modernizing its ICBMs and developing nuclear ballistic missile submarines. These tallies don't include more than 6,300 ballistic missiles that are beyond the control of established powers such as the U.S., Russia, China and NATO. In the 1970s only nine countries possessed ballistic missiles. Forty years later, the number exceeds 20, including potentially hostile regimes with ties to terrorist organizations.

That buildup makes missile proliferation among the world's greatest threats. Countries without ballistic missiles can now acquire them quickly and make them available to terrorist groups. Or North Korea, strapped for cash amid deepening sanctions, might sell surplus nuclear weapons to rogue states. "In light of the strategic threat presented by North Korea, defending the United States against intercontinental ballistic missiles remains USNORTHCOM's highest priority mission," Gen. Lori J. Robinson, then commander of U.S. Northern Command, testified before the U.S. Senate Armed Services Committee.



A Raytheon worker inspects a "kill vehicle" used to destroy intercontinental ballistic missiles in space. RAYTHEON

CONCLUSION

Beyond its material benefits, a reliable GMD system affirms the U.S. commitment to protect allies and deter adversaries anywhere in the world. It can deny hostile regimes the political benefits of having a weapon that can be used to threaten or blackmail peaceful nations. It can deter the buildup of nuclear missile systems by making them obsolete.

The U.S. has used economic sanctions and a cyber campaign to disrupt North Korea's missile system. While those tools have slowed North Korea's progress and generated attention and international pressure, the North Korean regime has yet to dismantle its nuclear arsenal. "We don't have to wait until they have an intercontinental ballistic missile with a nuclear weapon on it to say that now [the threat] is manifested completely," U.S. Defense Secretary James Mattis said.

AFP/GETTY IMAGES

ARTIFICIAL INTELLIGENCE COULD SAVE SHRINKING RAINFORESTS

Reuters

A new technique using artificial intelligence to predict where deforestation is likely to occur could help the Democratic Republic of the Congo (DRC) preserve its shrinking rainforest and cut carbon emissions.

The DRC's rainforest, pictured, the world's second-largest after the Amazon, is under pressure from farming, mining, logging and development. Protecting forests is widely seen as one of the cheapest and most effective ways to reduce the emissions driving global warming. Conservation efforts in the DRC, however, have suffered from a lack of precise data on which areas of the country's vast territory are most at risk of losing their pristine vegetation, said Thomas Maschler, a researcher at the World Resources Institute (WRI).

"We don't have fine-grain information on what is actually happening on the ground," he said.

To address the problem, Maschler and other WRI scientists used a computer algorithm based on machine learning, a type of artificial intelligence. The computer was fed inputs, including satellite data, detailing how the landscape in several regions had changed between 2000 and 2014.

The program analyzed links between deforestation and the factors driving it, such as proximity to roads or settlements, to produce a map forecasting future losses.

NORWAY HAS ELECTRIC PLANS FOR AUTONOMOUS SHIP

Agence France-Presse

Norway plans to launch the first autonomous and fully electric cargo ship in 2018, a feat the project's backers say will save 40,000 truck journeys per year.

Fertilizer company Yara International teamed up with industrial group Kongsberg to build the Yara Birkeland, which will haul fertilizer to three ports in southern Norway.

YARA INTERNATIONAL

With a range of more than 120 kilometers, the ship will haul 100 containers at a speed of 12 to 15 knots. Initially, the ship will be manned, but remote operation is expected to begin in 2019 and fully autonomous operation in 2020.

"Every day, more than 100 diesel truck journeys are needed to transport products from Yara's Porsgrunn plant to ports in Brevik and Larvik where we ship products to customers around the world," Yara Chief Executive Svein Tore Holsether said.

The switch is expected to reduce carbon dioxide emissions by 678 metric tons a year. The power used to charge the ship's batteries will come almost exclusively from hydroelectric plants.

A BABY STEP TOWARD HUMAN GENE EDITING

The Associated Press

For the first time in the United States, scientists have edited the genes of human embryos, a controversial step toward someday helping babies avoid inherited diseases.

MIT Technology Review reported in July 2017 that the experiment was just a scientific exercise: The embryos were not allowed to develop for more than a few days and were never intended to be implanted into a womb. Officials at Oregon Health & Science University confirmed the work took place there and said results eventually would be published in a journal.

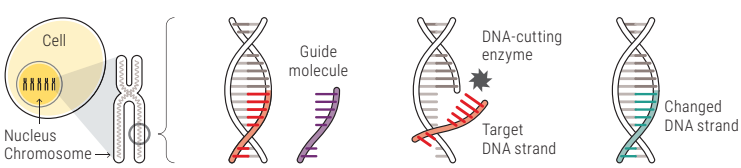
THE ASSOCIATED PRESS

The scientists used a technique called CRISPR/Cas9, which allows sections of DNA to be altered or replaced. The only similar previous work was reported in China.

Gene editing

A DNA editing technique called CRISPR/Cas9, works like a biological version of a word-processing program's find-and-replace function.

HOW THE TECHNIQUE WORKS



A cell is transfected with an enzyme complex containing:

Guide molecule

DNA-cutting enzyme

A specially designed synthetic guide molecule finds the target DNA strand.

An enzyme cuts off the target DNA strand.

The amended DNA strand repairs itself.

Source: Reuters

NORTHERN GUARD

Canada boosts defense spending to address an evolving threat environment

THE WATCH STAFF

When Canadian Defence Minister Harjit Sajjan announced Canada's new defense policy, analysts widely agreed the commitment to better training, improved troop support and new, modern equipment and weaponry are needed if the Canadian Armed Forces are to transition successfully into a force ready for future challenges. Gen. Jonathan Vance, chief of the Defence Staff, said it was a "great day to be in uniform." The plan, named Strong, Secure, Engaged, calls for an increase in defense spending of $13.8 billion Canadian (U.S. $10.8 billion) to $32.7 billion Canadian, or 73 percent, over the next 10 years.

The title of the new policy represents the three core objectives of Canada's defense doctrine: "Strong at home," to defend the Canadian homeland and protect Canadian citizens; "Secure in North America," reflecting Canada's defense partnership with the United States in the North American Aerospace Defense Command (NORAD); and "Engaged in the world," recognizing Canada's commitment to global peace and stability through membership in the NATO alliance and participation in United Nations peacekeeping and humanitarian operations.

> "If we are serious about Canada's role in the world, then we have to be serious about funding our military."
>
> **Harjit Sajjan, Canadian Defence Minister**

PARTNERSHIPS

As a measure of the importance of these partnerships, Canada consulted its allies and partner organizations throughout the policy development process. Minister of Foreign Affairs Chrystia Freeland said, "The ability to operate closely with allies and partners is an invaluable instrument of Canada's foreign policy" and noted that the policy will enhance joint endeavors against global security threats and in defense of the shared North American homeland.

This step is important in light of the heightened emphasis within NATO on increasing defense funding and shoring up member military capabilities, which was sparked by Russian aggression along the Alliance's eastern flank. Russia's illegal annexation of the Ukrainian territory of Crimea and military interference in eastern Ukraine have refocused post-Cold War NATO. The interference involved Russian

military units not wearing their insignia and Russian support to friendly rebels in eastern Ukraine and Crimea.

NATO Secretary-General Jens Stoltenberg reported that the alliance is boosting defense spending by 4.3 percent in 2017, adding that many members have committed to work toward the military spending goal of 2 percent of a country's gross domestic product. U.S. Secretary of Defense James Mattis applauded the new Canadian policy, saying it "demonstrates Canadian resolve," and Stoltenberg said that it "affirms Canada's unwavering commitment to NATO."

Increasing capabilities not only make Canada a more reliable and credible partner, as Sajjan pointed out, they also enhance Canadian sovereignty. "If we are serious about Canada's role in the world, then we have to be serious about funding our military," he said. Canada, however, "in terms of willingness to undertake missions and send Soldiers into harm's way, punches far above its modest budget weight within NATO," which amplifies its voice internationally, Sajjan said, according to *The Globe and Mail* newspaper.

As the policy document points out, a larger, more effective and better-equipped Armed Forces can better defend against any threats — existing, developing or yet unknown — to the nation's borders and interests. Of particular importance is Canada's offshore economic zone in the Arctic. An April 2017 report on military spending and capabilities from the Standing Senate Committee on National Security and Defence said Canada's top strategic challenge is defending sovereign rights in the Arctic. "The significant challenges involved in carrying out sovereignty protection are likely to grow as our Arctic becomes more accessible," the report states. "Effective protection of national sovereignty will require greater attention and investment in decades ahead" and will require a wide array of capabilities and "the ability to operate effectively on both land and on and under the sea in the Arctic."

As of August 2017, Canada was deploying about 800 troops in the fight against the Islamic State and about 200 providing training to Ukraine's military. Canada is also leading NATO's Enhanced Forward Presence battlegroup in Latvia, with 450 troops from the 1st Battalion Princess Patricia's Canadian Light Infantry.

A civilian Sea King helicopter lands on the flight deck of HMCS Montreal to pick up passengers during Neptune Trident 17-2 in October 2017.
LEADING SEAMAN DAN BARD/ROYAL CANADIAN NAVY

Christan Beaverho, who was participating in an aboriginal youth program of the Canadian Armed Forces, takes a break during an exercise at Rocky Point, Canadian Forces Base Esquimalt. The program is designed to build bridges into Canada's aboriginal communities and make young people aware of military and civilian careers in the Department of National Defence.

LEADING SEAMAN DAVID GARIEP/ROYAL CANADIAN NAVY

A CC-130 Hercules lands at Canadian Forces Station Alert in Nunavut during Operation Boxtop.
CPL. RYAN MOULTON/ CANADIAN ARMED FORCES

A CH-146 helicopter from 430 Tactical Helicopter Squadron flies over Ellesmere Island during Operation Nevus.
PETTY OFFICER 2ND CLASS BELINDA GROVES/CANADIAN ARMED FORCES

THE PLAN

People — Strong, Secure, Engaged aims to place an "unprecedented focus" on supporting troops and their families, from recruitment to retirement, and providing them resources they need to succeed. Gen. Vance called the plan's emphasis on the troops a big morale booster. "It's a good thing for a military to know its country has its back," he said.

The size of the active Regular Force will increase by 3,500 to 71,500, and the Reserve Force will grow by 1,500 to 30,000, with the reserves receiving new operational roles and improved integration with the Regular Force.

The plan includes tax relief for deployed service members, targeted recruiting for unique skills, greater diversity, significant investments in family resource centers, a comprehensive approach to health care and improved care for veterans. The aim is to improve recruitment and retention, while making the force ready and resilient.

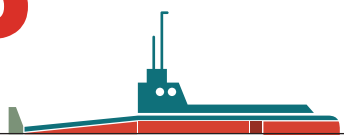
Weapons, equipment and technology — Canada's forces will be getting new weapons and equipment. The plan promises to supply the Royal Canadian Navy with 15 new Canadian surface combatant ships to replace its aging fleet of frigates and already retired destroyers, which will be "one of the largest acquisitions in Canadian shipbuilding history."

The Royal Canadian Air Force (RCAF) is slated to receive 88 advanced fighter aircraft, necessary to meet its obligations to NORAD and NATO, to replace about 80 CF-18 Hornets, which are rapidly approaching the end of their safe flight life spans. According to the Defense Industry Daily website, there is some debate over which fighters the RCAF will acquire. The previous government had committed to the CF-35 Joint Strike Fighter, but the new government has expressed doubts about the cost compared with European-sourced alternatives. Canada will also invest in restoration of aircraft, including the CP-140 Aurora anti-submarine and surveillance aircraft.

The Canadian Army will refurbish its land combat capabilities and vehicle fleets, acquire new armored vehicles, modernize its command and control systems and enhance the capabilities of light forces to better address modern challenges. Special Operations Forces have proven to be an invaluable tool in the fight against terrorism and other nonconventional threats. Special Operations Forces will become both larger and more agile.

Today's constantly evolving threat environment requires new and flexible approaches. Because intelligence and the real-time flow of information are key to success in modern military operations, Strong, Secure, Engaged commits Canada to acquire the latest in intelligence, surveillance and reconnaissance platforms, including next-generation unmanned aerial vehicles and space-based systems, as well as investment in intelligence experts. Cyber and space capabilities must remain at the cutting edge to defend against sophisticated threats, requiring highly skilled operators and enhancement of offensive and defensive cyber capabilities. To promote innovation in critical, cutting-edge research and development, $313 million Canadian is targeted for the Innovation for Defence Excellence and Security Program.

POLAR POLITICS AND PURSUITS



Nations are cooperating in the Arctic, but increasing militarization could put peace at risk

THE WATCH STAFF

Receding sea ice is ushering in a new resource race in the Arctic. Nations are maneuvering for control of the region, which holds rich deposits of oil, gas and minerals that are becoming newly accessible as the polar ice cap melts at an increasingly rapid rate. The melting ice, which is disappearing at about twice the pace of other spots on the planet, could also open shorter shipping routes between Western Europe and East Asia and expand commercial fishing and tourism opportunities. Some believe the Arctic Ocean will be ice-free during summer months as early as 2020 and year-round by 2050, unlocking potentially more than 20 percent of the world's petroleum reserves for extraction.

With spoils so alluring, many nations have increased research, exploration, development and other investment in the region as well as militarization, all of which present new quandaries and could threaten regional and global peace and security, some experts say.

"The increased commercial activity brings new challenges, including oil spill prevention, search and rescue, and potentially smuggling and immigration," says Dr. Michael Byers, an Arctic expert and international relations professor at the University of British Columbia in Canada.

Eight nations have territories in the Arctic — Canada, Denmark, Finland, Iceland, Norway, Russia, Sweden and the United States — but non-Arctic nations are seeking to assert influence in the region.

Russia, Canada and Denmark have formally claimed sovereignty over expanded sections of the Arctic seabed beyond their exclusive economic zones that extend 200 nautical miles from their shores. The overlapping claims, some of which date to before 1925 and include the North Pole, are yet to be resolved under the provisions of the United Nations Convention on the Law

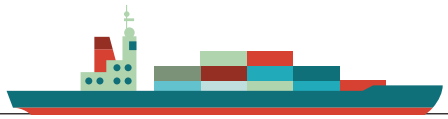
of the Sea (UNCLOS), which governs how disputes over maritime boundaries and territories are resolved and grants countries exclusive rights to harvest minerals and materials from underneath the seafloor of their continental shelves.

Control of the region could also potentially afford strategic military advantages. The U.S. has not made extended claims to the Arctic seabed but is contemplating how to conduct naval surface warfare in the changing Arctic.

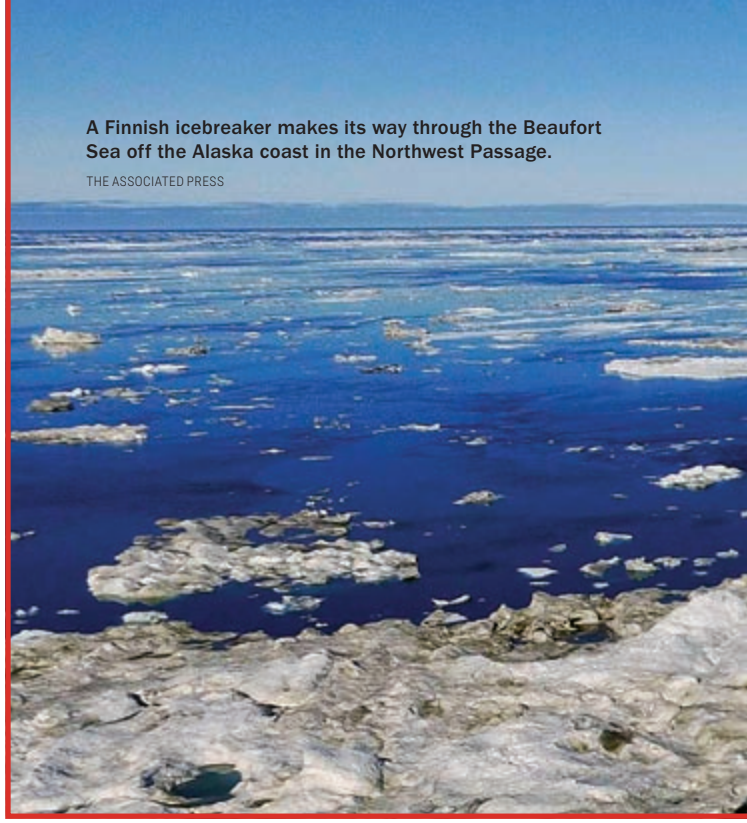
Arctic ice ranges up to 5-meters thick in places, making movement difficult. The ice is disappearing more quickly there than anywhere else on the planet, in part, because when the ice melts, the resulting water absorbs heat, speeding warming. Just slightly more than 20 percent of the Arctic's ice consists of multiyear ice that stays solid year-round, representing a drop of more than 50 percent from 20 years ago, according to the U.S. National Snow and Ice Data Center.

One of the key trade routes opening up, known as the Northern Sea Route, passes through Russian territory, running along its north coast from the Kara Sea to the Bering Strait. Ships can now connect for more days in the year between Russian Arctic ports and Norway. For example, transporting goods from Japan to the Netherlands using this route shaves almost 3,900 nautical miles off the journey via the Suez Canal, according to the Northern Sea Route Information Office in Murmansk, Russia. The other leading route, the Northwest Passage, which runs from the west coast of Canada to Finland, is about 1,000 nautical miles shorter than the conventional route through the Panama Canal.

Ships can now connect for more days in the year between Russian Arctic ports and Norway.



China has raised its profile in the Arctic in the past decade, given its interest in new commercial routes and increased activities there. China, Japan and South Korea have polar research programs with icebreaker facilities. For example, a Chinese research vessel called the Snow Dragon routinely explores along the U.S. continental shelf. China plans to upgrade its icebreaker fleet and develop technologies for exploiting Arctic natural resources such as deep-water drilling. A Chinese firm has purchased a U.S. $2.35 billion iron ore mining project in Greenland, which is an autonomous territory of Denmark, yet the consortium is awaiting better ore prices to develop it, Reuters reported. The mine has the capacity to produce 15 million tons of ore a year to ship to China.



A Finnish icebreaker makes its way through the Beaufort Sea off the Alaska coast in the Northwest Passage.

THE ASSOCIATED PRESS

Arctic Commons

The eight Arctic states created the Arctic Council in 1996 to promote cooperation, coordination and interaction on common Arctic issues such as sustainable development and environmental protection. The council also represents the 4 million-plus inhabitants who live north of 66 degrees latitude, about half of whom are Russian and 500,000 indigenous people.

The Arctic Council has granted observer status to 13 non-Arctic states: China, France, Germany, India, Italy, Japan, Netherlands, Poland, Singapore, South Korea, Spain, Switzerland and the United Kingdom. Another 26 intergovernmental, interparliamentary and nongovernmental organizations, including the newly added World Meteorological Organization and the National Geographic Society, enjoy observer status. The European Union and Turkey have also applied.

On passing the chairmanship from the U.S. to Finland in May 2017, then-U.S. Secretary of State Rex Tillerson said: "The Arctic Council, which recently celebrated its 20th anniversary, has proven to be an indispensable forum in which we can pursue cooperation. I want to affirm that the United States will continue to be an active member in this council. The opportunity to chair the council has only strengthened our commitment to continuing its work in the future."

Maintaining stability in the region remains critical for protecting economic prospects, experts say. "Military

and economic concerns are deeply intertwined in the Arctic," wrote Stephanie Pezard and several Rand Corp. colleagues in a March 2017 report, "Maintaining Cooperation with Russia."

"And ... these concerns can, at times," the report said, "lead to apparently disjointed Russian policies in the region."

More Militarization

Although there seems to be solid cooperation on Arctic Council matters and plenty of commercial opportunities for Arctic nations within uncontested areas of sovereignty where most oil and gas reserves lie, that hasn't stopped countries from militarizing the region. Russia is leading the military buildup, and most Arctic nations have bases there except Finland and Iceland.

Russia has the most military resources in the region with six military bases, 16 deep-water ports and 13 air bases and is continuing to reopen and build more bases there. In April 2017, Russia unveiled a 36,000-square-kilometer military complex in the Franz Josef Land archipelago called the Arktickhesky Trilistnik, or Arctic Trefoil. It's designed to protect Russian airspace and other Arctic assets. During its Victory Day Parade in May 2017, Russia showcased two new Arctic missile systems, the Tor-M2DT and Pantsir-SA.

Russia has the most military resources in the region with six military bases, 16 deep-water ports and 13 air bases and is continuing to reopen and build more bases there.

While the U.S.' interest in the Arctic is more peripheral, "the Russian Arctic is central to the Russian national identity," Ernie Regehr, senior fellow in Arctic security at The Simons Foundation in Vancouver, Canada, explains. "It has current and potentially much greater importance for the Russian economy, and the northeastern sea route is a major focus of Russian development of the region. The extraordinary Russian icebreaker fleet, its extensive system of search-and-rescue facilities, as well as its formidable military combat capability in the north, all speak to the importance Russia attaches to northern economic and resource development and to its commitment to protecting and advancing its interests there."

The increasing militarization of the region is causing concern. Russia is far from reestablishing its Cold War levels of military presence in the Arctic and is not likely to deploy Arctic-based assets in other potential contingencies such as disputes in the Baltic states, according to the findings of the 2017 Rand Corp. report. "Yet increased military presence — not

A Russian soldier stands near a military vehicle at the Nagurskoye base on the remote Arctic islands of Franz Josef Land.

REUTERS

just from Russia but also other Arctic countries — increases risk of collisions and accidental escalation," Rand's Pezard concluded.

"The Arctic Council, which focuses on environmental protection and sustainable development, has continued to operate normally despite increased tensions between NATO and Russia. Cooperation on search and rescue is also continuing," said Byers, who is author of *International Law and the Arctic*, published in 2013 by Cambridge University Press. "However, communication between the Russian military and other Arctic militaries has broken down, which creates unfortunate risks of misunderstanding and accidental conflict."

With the ice melting and Russia and China increasing investments and presence in the Arctic, there remains no mechanism to address security issues in the region, including this militarization trend, experts explain. The founding charter of the Arctic Council forbids the body from discussing security matters, leaving it in the hands of individual nations to address military developments through bilateral channels. NATO and Russia do not discuss developments in the Arctic. Without a mechanism, military movements in the Arctic could be misinterpreted or cause a military incident, Heather Conley, senior vice president at the Center for Strategic and International Studies (CSIS), told The Watch.

Ensuring Cooperation

To be sure, all Arctic nations agree that international cooperation is key for nations to realize the economic potential and ensure prosperity and security of the far north, yet much work remains to achieve such common goals. Finland, as chair of the Arctic Council, aims to focus on the core pillars of the organization, which include enhancing biodiversity, assessing climate change, sustainable development, and protecting the

marine environment. Yet some analysts are pushing for stronger mechanisms to resolve security-related issues. "Without predictability, transparency and trust, there will be no international cooperation in the Arctic," Conley concluded in a 2015 CSIS report titled "The New Ice Curtain: Russia's Strategic Reach to the Arctic."

The Simons Foundation's Regehr agrees. "It is critically important to develop an institution or mechanisms for regular, ongoing consultation on mutual security interests, concerns and enhancements. Whether that can happen within the scope of the Arctic Council is an open question. One huge advantage of bringing security concerns and considerations into the Arctic Council is that indigenous communities would then have a continuing place at the table for security deliberation."

Ironically, during establishment of the Arctic Council, the U.S. wanted it to avoid military discussions out of concern it would promote militarization of the region. But two decades later, the Arctic is becoming militarized and the international community lacks a forum to discuss security issues. Many experts, including Conley, would like to see the Arctic Council develop a nonbinding political statement to serve as a code of military conduct in the Arctic. For example, such a declaration would mandate that countries notify each other 21 days in advance of military exercises involving 20,000 troops or more and invite observers.

Moreover, Russia's cooperation in the Arctic should not be taken for granted, according to the Rand report. "If economic ambitions grow increasingly out of reach — for instance, because of low hydrocarbon prices, capital flight and/or the loss of foreign investment and expertise — Russia could have less of an incentive to cooperate and might engage instead in inflammatory actions and rhetoric."

A disruption of vital resources and routes in the Arctic could trigger military disputes, some experts warn. Additionally, the Arctic Council has opened pathways for foreign influence, especially through investment and expertise. The convergence of territorial disputes, newly emerged commercial shipping lanes and natural resource exploitation could increase tensions in the region, if recent interactions in the South China Sea indicate what's to come.

Although neither China nor any other country has built and armed artificial islands in the Arctic, territorial disputes could intensify. "As I look at what is playing out in the Arctic, it looks eerily familiar to what we're seeing in the East and South China Sea," Adm. Paul Zukunft, then commandant of the U.S. Coast Guard, said at a CSIS-sponsored event in Washington, D.C., in August 2017, according to Defense One, an online security publication.

> "As I look at what is playing out in the Arctic, it looks eerily familiar to what we're seeing in the East and South China Sea."
>
> **Adm. Paul Zukunft,** then commandant of the U.S. Coast Guard

To avoid any duplication of the gradually escalating tensions in the South China Sea, Zukunft urged the U.S. to ratify the 1982 UNCLOS Treaty, under which the Philippines, for instance, filed suit against China for violating its sovereignty.

The U.S. should also increase its Arctic footprint, he and other analysts assert. "Obviously, we've seen what's happened in the East/South China Sea — even though the U.N. tribunal found in favor of the Philippines, it has not altered the behavior of China," Zukunft said, Defense One reported. "We can write great policy, but if you do not have presence to exert sovereignty, you are really nothing more than a paper lion," he told Reuters.

NATO's Strategic Foresight Analysis report also cautions that mounting resource competition could contribute to instability in the region in future decades.

For now, however, most of the Arctic's territorial disputes are among NATO allies. And overall militarization of the Arctic has not approached the levels of the Cold War. Moreover, the vast expanses of the Arctic and its extreme weather offer natural defenses to its inhabitants, the University of British Columbia's Byers says. And little has changed to shorten the great distances between outposts and treacherous climate conditions in the past decade. As Gen. Walter Natynczyk, Canada's then-chief of the defense staff, said in 2009: "If someone were to invade the Canadian Arctic, my first task would be to rescue them." ■

NORAD'S MARITIME MISSION

Command defends against potential threats from the sea

NORAD MARITIME TEAM

The end of the Cold War did not diminish the importance of the North American Aerospace Defense Command's (NORAD) aerospace warning and control role, and the events of 9/11 focused leaders on potential threats that resulted in adding maritime warning to NORAD's responsibility. The complexity of maritime security and the defense of North America stems from the numerous threat vectors encompassing millions of square miles of ocean. The challenge to the security and defense of Canada and the United States is global. Achieving maritime domain awareness is crucial, and no single organization possesses the intelligence and information necessary to accomplish the maritime mission without support from others. Additionally, the sharing of information and intelligence among partners is a significant challenge requiring approved information-sharing agreements, trust between organizations and an understanding of information requirements among maritime agencies. Protecting the maritime approaches and inland waterways of North America requires the development of a shared understanding and awareness of maritime activities.

Maritime threats to Canada and the United States range from small boats operated by transnational criminals to nation state competitors. Cooperation is essential to identify, warn against and counter the complete maritime threat spectrum. In this complex environment, NORAD, through its maritime warning mission, fills a critical need to define and transmit maritime threats to the Canadian and U.S. governments.

EVOLVING MARITIME MISSION

NORAD, based in Colorado Springs, Colorado, is one of the most enduring military partnerships of the post-World War II era. NORAD authorities and responsibilities were established in 1958 through a formal agreement between the governments of the U.S. and Canada. The agreement provides binational aerospace warning and aerospace control to alert and, if necessary, defend North America against threats from strategic long-range aviation, intercontinental ballistic missiles and asymmetric threats in the air. Immediately after 9/11, then-U.S. Secretary of Defense Donald Rumsfeld directed enhanced military cooperation between Canada and the U.S. This led to a proposal to expand NORAD beyond its aerospace missions into the maritime domain. An agreement to expand the mission to include maritime warning was formalized with the signing of the 2006 NORAD agreement.

NORAD is uniquely positioned as a binational command with a global area of responsibility. The NORAD commander is directly responsible to both the Canadian and U.S. national security establishments. For threats originating in the maritime domain, maritime warning is NORAD's responsibility, while maritime homeland defense is a national responsibility assigned to U.S. Northern Command (USNORTHCOM) and Canadian Joint Operations Command (CJOC). The NORAD Maritime Division executes the maritime warning mission through a core group of personnel from the Royal Canadian Navy and the U.S. Navy augmented by civilians and contractors. NORAD does not own maritime sensors nor does it monitor a raw maritime radar picture. Rather, NORAD personnel monitor the common operating picture provided by Canadian and American sources, review operational and intelligence information from numerous sources and initiate information sharing. In addition, two NORAD maritime division personnel work in the NORAD and USNORTHCOM Joint Intelligence Operations Center to provide a dedicated source of maritime intelligence.

THREE PILLARS OF MARITIME WARNING

The NORAD agreement provides NORAD with the authority to communicate information on North American

maritime threats to the U.S. and Canadian governments. Response to a specific threat by the appropriate command, department and/or agency remains a national responsibility. The NORAD Terms of Reference, approved by the Canadian chief of defence and the chairman of the U.S. Joint Chiefs of Staff, specify the tasks that support the accomplishment of the maritime warning mission. The maritime warning mission is supported by three pillars:

- Participate in the overall maritime information sharing network.
- Develop a comprehensive shared understanding of maritime activities.
- Communicate maritime warnings to the governments of Canada and the U.S. for response by the appropriate national commands and/or departments and agencies.

INFORMATION SHARING

Information sharing is the foundation of the maritime warning mission. NORAD leverages existing support relationships to formalize and develop habitual routine information and intelligence-sharing practices; identifies and addresses information and intelligence gaps, seams and barriers; and develops new mutual support relationships to advance the mission. NORAD is supported by CJOC, USNORTHCOM, U.S. Africa Command, U.S. European Command, U.S. Pacific Command, U. S. Southern Command and U.S. Strategic Command. Conversely, NORAD's maritime warning mission supports these same agencies in the execution of their own maritime missions. These military agencies represent only a limited section of the maritime community of interest. In total, the stakeholders in the maritime community are composed of over 70 military, civilian (tribal, local, state and federal) and private-sector agencies that span security, law enforcement and defense sectors. Many of these organizations have their own intelligence-producing directorates to support their mission in the maritime domain. Some of NORAD's maritime warning responsibilities are to formalize direct relationships, participate in maritime domain awareness forums and map out information- and intelligence-sharing relationships throughout the maritime community.

A significant challenge to information and intelligence sharing is the restriction in sharing classified information, technical network barriers and policies that inhibit information flow. As a binational command, NORAD is in a unique position to facilitate information sharing between Canada and the U.S. As part of the mission to share information, NORAD is also tasked with identifying and resolving information-sharing challenges in the maritime domain.

Overlapping authorities in the maritime community create a complex environment. In the United States, the U.S. Customs and Border Protection National Targeting Center runs a worldwide program that ensures proper screening of inbound maritime. However, according to federal counterterrorism policy, the FBI is the lead agency for all counterterrorism, including maritime threats. Closer to home, the U.S. Coast Guard is engaged daily in a broad spectrum of operations that include law enforcement, regulation and defense. The U.S. Maritime Administration works with the shipping industry to identify threats worldwide and communicate advisories and alerts, while the U.S. State Department and Global Affairs Canada review and approve operations of foreign military and research vessels in economic exclusion zones and territorial waters. Within Canada, Canadian Marine Security Operations Centres on the East and West coasts include members from Transport Canada, the Canadian Coast Guard, the Royal Canadian Mounted Police and the Department of National Defence, who work to identify threats on the Great Lakes, inland waterways and the Canadian maritime approaches. Additionally, the World Health Organization is charged with providing information on infectious pathogens (e.g., Ebola), which may be spread by maritime cargo and passengers. These myriad organizations demand an overarching entity empowered to ensure efforts are coordinated and information is shared.

The NORAD Terms of Reference authorize direct liaison with any external department or agency outside of the U.S. Department of Defense (DOD) or Canadian Department of National Defence to share information and intelligence quickly among the maritime community of interest. NORAD maritime warning, through the initiation of a classified conference call, can link multiple Canadian and U.S. interagency operations centers via a secure network to gather information on a developing maritime threat or quickly disseminate information. NORAD receives information from the Global Maritime Operational Threat Response Coordination Center, which coordinates a U.S. response to maritime events among multiple federal departments and the White House staff.

NORAD also participates in conferences and working groups focused on submarine and undersea research threats, Arctic operations and surveillance capabilities, and policy development. To facilitate routine and habitual information sharing, NORAD Maritime leads and participates in several regularly occurring maritime information and intelligence synchronization events. Each month, NORAD leads the Maritime Domain Awareness Synchronization secret video teleconference (SVTC), a venue that allows participants from Canada and the U.S. to discuss vessels of interest, future operations and past events and advertise maritime initiatives. Additionally, NORAD participates in the Port Security Group, Atlantic and Pacific Submarine Operations/Intelligence boards, vessel of interest SVTCs and human smuggling VTCs.

NORAD is a tri-chair of the Maritime Stakeholders Conference (MSC) with Transport Canada's Interdepartmental Marine Security Working Group, and the National Maritime Intelligence Integration Organization (NMIO). This annual event gathers maritime domain awareness (MDA) representatives from both nations to share information, champion efforts to

U.S. Coast Guard members practice shooting aboard HMCS Moncton, a vessel designed for coastal patrol, minesweeping and training.

ROYAL CANADIAN NAVY

build MDA capacity and promote information sharing. A noteworthy effort backed by the MSC was the expansion of radar coverage in Puget Sound, which straddles the U.S. and Canadian border. The expansion supports binational law enforcement along with the enhancement of information sharing between Canada and the U.S. This conference provides focus for the maritime community participants, including policy recommendations.

In addition to sharing operations and intelligence, NORAD provides its knowledge and perspective to assist agencies in developing maritime policy. Recently, NORAD worked with the DOD executive agent for MDA, who is leading the implementation of the National Vessel of Interest (VOI) lexicon. It provides a standardized language when classifying maritime threats based on threat category, specific threat details and threat level. The VOI lexicon was initially developed in 2007 for use by NORAD and USNORTHCOM to standardize terminology on maritime threats. Over the last decade, NMIO, as the U.S. Office of the Director of National Intelligence's maritime manager, has further refined the lexicon and broadcast it to a larger audience. Once the policy and concept of operations for national use of the VOI lexicon is completed, it will enable all DOD departments and agencies to delineate specific reporting criteria and track threats using a common language.

DEVELOPING SHARED UNDERSTANDING

The second pillar of NORAD's maritime mission is to develop a comprehensive shared understanding of maritime activities. This task involves processing and disseminating intelligence data and operational information to gain maritime awareness. Furthermore, it involves validation, characterization and assessment of a potential attack or actual attack against North America by traditional or asymmetric maritime threats.

Developing a common operational picture is a constant challenge because multiple classified and unclassified systems form the picture of surface and subsurface activity. Global Command and Control System, SIPR Google Earth, Agile Client, Situational Awareness Advanced Analytics, Automatic Identification System feeds and space-based systems provide various pieces of the MDA puzzle. There are dozens more. Layering these feeds and combining more information and intelligence produces a truly comprehensive maritime picture.

COMMUNICATING WARNING

The third pillar within NORAD's maritime warning is communication. Sharing information and developing MDA is important, but the effort is futile if NORAD cannot communicate maritime warnings to the Canadian and U.S. governments. Maritime warning is subdivided into maritime advisories and maritime warnings, depending upon a variety of criteria, including the capability of the threat, its location and assessment of its intent. Regardless of which designation is used, advisories and warnings are promulgated through message traffic and classified email to inform senior decision-makers in both governments of specific threats or potential attacks. NORAD's classified conference call may also be used to promulgate the contents of the advisory or warning.

In the absence of a global synchronizing agency specifically authorized to develop a comprehensive maritime picture, NORAD's greatest value is to provide redundancy in assessing the maritime picture and ensure that information and intelligence are shared among a diverse group of binational participants. NORAD is uniquely positioned as a member of the "Tri-Commands," which includes USNORTHCOM and CJOC, to champion the cooperation and information sharing necessary to ensure the safety and security of North America from all maritime threats.

WELCOME WARRIORS

THE WATCH STAFF

From fierce hurricanes to deadly quakes, USNORTHCOM rises to the challenge

For many North Americans, the summer of 2017 was one better forgotten. Lightning-quick wildfires scorched more than 8 million acres of the American homeland — from the wilderness of Wyoming to the wine region of California. Deadly hurricanes battered Florida, Puerto Rico and Texas, leaving thousands homeless and without water or power. Add to that three deadly earthquakes in Mexico in a little more than two weeks, and the business of providing disaster relief proved logistically daunting.

That job — responding to each disaster by supporting civil authorities with manpower, gear and lifesaving supplies — fell to U.S. Northern Command (USNORTHCOM), the same military command responsible for protecting North America from attack. Whether the command was flying fuel, food and Soldiers to far-flung places such as Key West and Puerto Rico or sending search-and-rescue teams to hunt for survivors in the rubble of Mexico City, USNORTHCOM relied on years of planning and lessons learned from Hurricane Katrina to meet the challenges.

"We've come a long way since Hurricane Katrina, and we've learned a lot from Superstorm Sandy [in 2012]," Lt. Gen. Reynold N. Hoover, deputy commander of USNORTHCOM, said at the Gen. Bernard W. Rogers Strategic Issues Forum hosted by the Association of the U.S. Army's Institute of Land Warfare in April 2017.

DISASTER RELIEF PLAYBOOK

Americans devastated by the barrage of disasters in 2017 received relief more quickly in many cases, thanks to those lessons learned in 2005, when USNORTHCOM was in its infancy and Katrina battered the U.S. Gulf Coast. The command, which turned 15 years old in 2017, has fully integrated its relief efforts into "playbooks" developed with the Federal Emergency Management Agency (FEMA). The playbooks script mission assignments and resource coordination.

They simulate scenarios ranging from an earthquake and tsunami on the West Coast to the detonation of an improvised nuclear device on the East Coast. "With this playbook, we know what FEMA's going to ask for in the first minutes of the operation," Hoover said in a story on the Army institute's website. He emphasized that all disasters are "inherently local" and that

A massive wildfire leaves the smoldering remains of cars and homes in Glen Ellen, California. Tens of thousands of acres and dozens of homes and businesses burned in Napa and Sonoma counties.
AFP/GETTY IMAGES

USNORTHCOM's role is not to assume command in a crisis but to support governors, state emergency managers, local officials, FEMA and other federal agencies.

No mock scenario, however, forecast exactly what happened in 2017.

TAKING IT TO THE LIMIT

The scope of the disasters was jaw-dropping. Hurricane Harvey, which poured up to 152 centimeters of rain in some parts of Southeast Texas and resulted in more than 80 deaths, made landfall as a Category 4 hurricane on August 25, 2017.

Texas Gov. Greg Abbott estimated the damage to his state could hit U.S. $180 billion, making Harvey one of the most destructive storms in U.S. history. More than 210,700 homes were damaged or destroyed, The Associated Press (AP) reported, and saving the lives of the people trying to escape rising water required precise coordination and as much hardware as USNORTHCOM, headquartered at Peterson Air Force Base in Colorado Springs, Colorado, could muster.

State and federal agencies conducted more than 122,300 rescues and evacuations. Those included more than 34,000 by the Texas National Guard and other state military forces and more than 11,000 by the U.S. Coast Guard. In Houston, police performed 5,000 water rescues, AP reported, and USNORTHCOM rescued more than 3,000.

To respond more efficiently, USNORTHCOM prepositioned resources. In less than a week after Harvey's landfall, the command had already deployed 73 helicopters, three C-130 transport planes and eight teams to conduct search-and-rescue missions and evacuations. The command worked with the Defense Logistics Agency, which by August 31, 2017, had delivered 600,000 gallons of fuel to military bases in Texas and 45,000 gallons of aviation fuel to enable the U.S. Coast Guard to conduct rescues. That's in addition to USNORTHCOM's delivery of more than 100 military vehicles, tens of thousands of sandbags and many high-capacity electrical generators.

In addition to FEMA and USNORTHCOM, other federal agencies aiding the effort included the Department of Health and Human Services, Geological Survey, Department of Housing and Urban Development, Army Corps of Engineers, Environmental Protection Agency, Department of Energy, Department of Defense, Small Business Administration, Civil Air Patrol, Department of Agriculture, General Services Administration, Centers for Medicare and Medicaid Services, and Department of Transportation.

The demands posed by the record flooding were a summer's worth of work, but the disasters had just begun. A little more than two weeks after Harvey's arrival, Hurricane Irma was spinning at Category 3 strength when it raked the Florida Keys before making landfall near Marco Island in southwest Florida at the same intensity on September 10, 2017.

For Irma, USNORTHCOM called on U.S. Marines in the region, Army troops from North Carolina and ships from the Atlantic fleet to provide supplies and serve as floating medical clinics. As U.S. Navy ships delivered food and water to Key West, Marine helicopters evacuated patients from the U.S. Virgin Islands. USNORTHCOM provided aerial and ground reconnaissance and assessment as well. At the peak of relief efforts, the Defense Logistics Agency was supplying 1.2 million meals a day to weary Floridians.

Irma's signature impact was a damaged power grid. A day after landfall, 7.3 million people were without power across multiple southeastern states, Reuters estimated. USNORTHCOM responded by sending fuel to a National Guard base near Starke, Florida, to help utility crews restore power.

"The team is doing awesome work and is having a direct impact on the relief efforts," U.S. Air Force Brig. Gen. Martin Chapin, then energy commander of Defense Logistics Agency, said after Irma's landfall. "Every time a utility truck goes out and power is back on for citizens, it's because we provided them fuel, and everyone who is supporting this effort should be proud."

With two storms under its belt, USNORTHCOM faced yet another test. Hurricane Maria's destruction of Puerto Rico was devastating. After the Category 5 hurricane's September 20,

AFP/GETTY IMAGES

2017, landfall, 55 percent of the Puerto Rico's 3.5 million people had no drinking water, and 95 percent of its 1.57 million electricity customers had no power. Areas of the island faced many months without power, said Lt. Gen. Todd T. Semonite, commander of the U.S. Army Corps of Engineers.

In the first days after the storm, lifesaving supplies topped the list for responders. FEMA sent more than 4.4 million meals and 6.5 million liters of water to Puerto Rico by early October. More than 12,600 federal employees from 36 agencies were on the ground in Puerto Rico and the U.S. Virgin Islands, according to FEMA.

To lead the relief effort, the Pentagon put Lt. Gen. Jeffrey Buchanan in charge of all military hurricane response efforts in Puerto Rico. The command worked with local, state and federal authorities to restore power to hospitals and then gas stations to fuel relief operations and boost daily commerce.

"Everything has been prioritized. We went to hospitals first. Now we're on gas stations," then-Acting Homeland Security Secretary Elaine Duke told reporters. "This is a conscious effort to make sure we don't have loss of life."

"It has been amazing to see both sides of the evolution of how we, as a federal government, respond to disasters."

Coast Guard Capt. Scott Langum

A Texas National Guardsman carries a woman from her flooded home in Houston, Texas, after Hurricane Harvey soaked the city.
AFP/GETTY IMAGES

USNORTHCOM strategically located ships to arrive as quickly as possible. Those ships included the USNS Comfort, a medical treatment ship, as well as the USS Kearsarge, USS Oak Hill, USS Wasp and the USNS Supply. The military also sent eight C-17 aircraft. In addition to treating dozens of patients, the USNS Comfort hosted a medical summit with local and federal officials, including Puerto Rico Gov. Ricardo Rossello and U.S. Surgeon General Dr. Jerome Adams, to coordinate humanitarian aid.

Restoring power fell to the Corps of Engineers, which by October 5, 2017, had installed 27 generators at critical facilities. Schools were opened as food distribution centers for residents, and more than U.S. $2.2 billion in grants and low-interest loans were made available to Puerto Rico residents, FEMA reported.

EARTHQUAKES AND WILDFIRES

After already responding to wildfires across the American West and major hurricanes, USNORTHCOM received a call from officials in Mexico City, who were responding to a severe earthquake that toppled buildings, trapped people in the rubble and eventually resulted in 370 deaths.

A U.S. Air Force C-17 flew 60 search-and-rescue experts and their dogs to Mexico City to help locate survivors. The Air Force followed that by sending relief supplies aboard other planes.

"We're fueled by caffeine and inspired by the actions of others," Coast Guard Capt. Scott Langum, a future operations director with the command, told *The Gazette*, a Colorado Springs newspaper. Langum said the intensity and scope of the disasters in 2017 provided USNORTHCOM with unprecedented challenges. "It really isn't like anything we've experienced," he told the newspaper.

Even before the rain, winds and earthquakes, the year started with devastating wildfires. More than 8 million acres, 500 homes and other structures were burned in the United States, according to the U.S. Fish and Wildlife Service. The bulk of those fires occurred in western states, with California, Montana and Idaho hit the worst.

Civilian resources weren't enough to contain the blazes, so FEMA asked the Pentagon for help. USNORTHCOM sent C-130 firefighting planes and Soldiers from Fort Lewis near Tacoma, Washington, to support local and state authorities.

Overall, the summer of 2017 proved that USNORTHCOM's disaster-response skills have matured. During Hurricane Katrina in 2005, Langum piloted a Coast Guard rescue helicopter, *The Gazette* reported. By 2017, he was helping lead USNORTHCOM's entire hurricane rescue efforts. "It has been amazing to see both sides of the evolution of how we, as a federal government, respond to disasters," he said.

LIBYA

TRIPOLI ASKS ITALY TO HELP FIGHT TRAFFICKERS

Agence France-Presse

Libya's United Nations-backed prime minister, Fayez al-Sarraj, has appealed to Italy to send ships into Libyan territorial waters to combat human trafficking.

Sarraj sent a letter requesting that "the Italian government provide the technical support of Italian naval units in the joint struggle in Libyan waters against human traffickers."

Then-Italian Prime Minister Paolo Gentiloni said the Ministry of Defense was considering the request, and "the options will be discussed with the Libyan authorities and the Italian Parliament."

Should Italy respond positively, "as I believe is necessary, it could be a very important development in the fight against people trafficking," he said.

The move would reduce the number of migrant boat departures from the coast of crisis-hit Libya and ease the strain on Italy, which has struggled to house thousands of people rescued at sea.

Sarraj said, "We need to do more so that our Coast Guard can fight illegal immigration and ensure that we have advanced technologies to control our coasts."

REUTERS

ROMANIA

AGENCE FRANCE-PRESSE

DEFENSE MINISTER CONFIRMS U.S. MISSILE DEAL

The Associated Press

Romania's defense minister said in July 2017 that the country intends to buy Patriot missiles worth U.S. $3.9 billion from the United States.

Then-Defense Minister Adrian Tutuianu estimated Romania would begin paying for the missiles after Parliament passed a law to allow the acquisition.

The U.S. State Department approved the sale, saying it would help to "improve the security of a NATO ally … that is an important force for political stability and economic progress within Europe."

The State Department said the missile system would strengthen Romania's homeland defense and deter regional threats, increase the defensive capabilities of the Romanian military and shield the NATO allies who often train in Romania.

The U.S. increased its presence in Eastern Europe with regular training exercises to reassure NATO's European allies after Russia annexed Ukraine's Crimean Peninsula in 2014.

ESTONIA

WORLD'S FIRST VIRTUAL DATA EMBASSY

Agence France-Presse

Cyber-savvy Estonia is taking a step forward in global technology, with the small Baltic state opening the world's first data embassy in Luxembourg early in 2018.

The heavily protected server room contains important Estonian e-government records, so the NATO and eurozone member can access them even when systems are inoperative at home.

"Data security and cyber security are generally crucial from the perspective of both people's confidence and the functioning of services," Estonian Prime Minister Juri Ratas said in June 2017.

Ratas released the statement after signing an agreement with his Luxembourg counterpart, Xavier Bettel, on housing Estonian data there.

The country of 1.3 million people has been dubbed E-stonia for being a technological trailblazer. In 1991, after five decades of Soviet rule, Estonia opted to go high-tech as fast as possible. Its adoption of advanced technology has outpaced that of other members of the European Union, which it joined in 2004.

The Baltic state has made most public services accessible at a special state portal and pioneered e-voting in 2005.

Its capital, Tallinn, is home to the NATO Cooperative Cyber Defence Centre of Excellence, where data experts from Europe and the United States work to protect the information networks of the alliance's 29 member states.

The data embassy in Luxembourg will back up government records regarding taxes, land, businesses, identity documents, pensions, legislation and the census.

"The virtual data embassy's main goal is to guarantee the country's digital continuity: the capacity to start the systems when necessary and retrieve data from externally stored versions," said Emilie Toomela, spokeswoman for the Ministry of Economics and Communication.

"Luxembourg was chosen for the state-owned high-security, Tier 4 certified data centers the likes of which Estonia does not have and also because Luxembourg is ready to guarantee diplomatic privileges to Estonian data and infosystems," she added.

CZECH REPUBLIC

ARMED FORCES TO BOOST NUMBERS BY 30 PERCENT

Agence France-Presse

The Czech Republic announced it will increase the size of its Armed Forces by 30 percent after the government approved raising defense spending.

Then-Defense Minister Martin Stropnicky said the number of people in the Armed Forces would rise from about 23,000 to 30,000 "within the next five to seven years."

"The Czech Army is currently among the smallest in Europe in relation to its population," he said. The Czech Republic has a population of 10.5 million.

"The list of wanted professions is very wide," he said. "We need drivers as much as we need surgeons and pilots."

In July 2017, the government approved the purchase of 80 Italian-made light armored vehicles and 62 multirole armored vehicles, sourced from French and Czech companies, for a total cost of U.S. $410 million.

AFP/GETTY IMAGES

MILITARY MOUNTAINEERS

Nepalese, U.S. partners share cold facts about high-altitude operations

THE WATCH STAFF

When the doors finally opened after a 2½-hour air mission, 128 paratroopers braced for the jump of their lives. They were jumping from an altitude of about 400 meters into an Arctic no man's land — a place called Deadhorse, Alaska — wearing more than 90 kilograms of kit that included snowshoes, weapons and supplies.

"As the paratroopers exit, it's [minus 76 Celsius] for 2 1/2 seconds until their chute opens," said Maj. Gen. Bryan Owens, then commanding general of U.S. Army Alaska (USARAK). "Once their chute opens, it's [minus 53 Celsius] to the ground, and in four hours of operations on the ground, it's [minus 53 Celsius]. It was incredible."

The Soldiers from the 4th Brigade Combat Team (Airborne), 25th Infantry Division who braved the deadly cold were participating in Spartan Pegasus, an annual cold-weather training exercise in frozen tundra just a few kilometers from the Arctic Ocean. Training lessons learned during the exercise, which in 2017 was designed to retrieve a downed satellite, and at courses in the Northern Warfare Training Center in Black Rapids, Alaska, can mean the difference between a successful mission and tragedy. In subzero temperatures, the smallest mistakes can be lethal — such as touching a weapon or brushing up against skiing equipment with bare skin.

> Extensive training, the best equipment and savvy leadership are keys to success. "There's a difference between surviving in a cold region and thriving."
>
> **Maj. Gen. Bryan Owens, U.S. Army**

"Something as simple as skin-to-metal contact is deadly," Owens said during the Association of the U.S. Army Institute of Land Warfare's Land Forces of the Pacific Symposium and Exhibition (LANPAC) in Honolulu, Hawaii. "That will give you instant frostbite. You've got to be careful not to have any of the metal parts touch your skin."

PACIFIC PARTNERS

From North America's tallest peak, Denali, to the majestic Himalayas of Asia to the Andes in South America, many of these military mountaineering and cold-weather lessons are universal. USARAK teams up with Indo-Pacific countries to expose Soldiers to new techniques and challenging environments. USARAK's main mountaineering training partners in the region are Chile, India, Japan, Mongolia and Nepal. The combined training and the sharing of tactics and techniques to perform in subfreezing temperatures better prepare Soldiers from the U.S. and its partners to defend their respective homelands.

"We look for similarities with our partners in geography and similar challenges that they have," Owens said. "That allows us to share best practices. It allows us to build on each other's strengths. That's been very beneficial for us."

The exchange also has benefited Nepal, which is home to Mount Everest and some of the world's most unforgiving terrain, said Nepal's chief of Army, Gen. Rajendra Chhetri.

In a country where 80 percent of the landscape is mountainous, thriving in high-altitude environments — everything from conducting military operations to rescuing climbers from Everest — is part of everyday life for Nepalese Soldiers, Chhetri said. "There are many challenges we have to face while operating in altitude," Chhetri said. "There are health hazards if you don't properly dress up. With the low oxygen level, you can feel altitude sickness.

> "The ability to dress properly, layer and shed properly so you don't end up perspiring in a cold-weather environment. You don't want to perspire in a cold-weather environment. That's very dangerous."
>
> **Maj. Gen. Bryan Owens, U.S. Army**

If you don't have proper gear, frostbite will affect you."

The Nepalese Army shares these lessons with its many partners. It has been operating the Nepal Army's High Altitude and Mountain Warfare Training Academy for more than four decades, Chhetri said. Neighboring Indo-Pacific countries, including Bangladesh, China, Pakistan and Sri Lanka, send their Soldiers to train there, as do the United States, Canada, the United Kingdom and other European countries. "We opened up our altitude warfare school to international students, including U.S. students," Chhetri said. "The U.S. is a regular participant in that course."

While Nepal's Soldiers are extremely experienced at operating in high altitudes, a Mongolian military leader said his country shares insights into these military-to-military exchanges that are derived from centuries of conducting operations in austere environments.

Lt. Col. Shinebayar Dorjnyam, deputy commander of the Mongolian special forces, said through a translator during LANPAC that he attended entry-level high-altitude training in Alaska in 2015 and was impressed with the new technology supplied by the U.S. Army.

While the U.S. provided top technology, the deputy commander said, his Soldiers possess their own secrets of the trade. "We are unique because we still maintain our nomadic lifestyles," he said. "We preserve the skills that we have with that. We know how to make fire, adapt and adjust — free of technology."

A U.S. Marine secures his platoon during a cold-weather exercise in Norway.
NORWEGIAN ARMED FORCES

A U.S. Army paratrooper pauses during a break in live-fire training at Joint Base Elmendorf-Richardson, Alaska.

ALEJANDRO PENA/U.S. AIR FORCE

NORDIC ALLIANCE

The U.S. Army isn't the only service engaged in cold-weather training exchanges. U.S. Marines are teaming up with a NATO ally to master cold-weather operations and military mountaineering to improve homeland defense. The Marine Rotational Force-Europe arrived in central Norway in January 2017 — the first foreign troops to deploy in Norway since 1949.

As part of their cold-weather training, they learned how to dry their sweat-soaked clothes using their own body heat, how to consume every ounce of energy from a slaughtered reindeer by drinking its blood and eating its meat, and how to melt and boil snow to prepare freeze-dried food.The deployment is part of a bilateral agreement between Oslo and Washington.

THRIVING IN SUBZERO

While survival is difficult in subzero temperatures, Soldiers can't afford to set the bar that low. They train to conduct military operations in environments many people will never experience, Owens said. "A lot of people think you can take a very highly trained unit and put them into extremely cold weather, and they'll sort it out. They'll be able to function there," he said. "That is not the case."

Extensive training, the best equipment and savvy leadership are keys to success. "There's a difference between surviving in a cold region and thriving," he said.

At the Northern Warfare Training Center, Soldiers are taught basic military mountaineering as well as advanced cold weather skills, which involve heat management — "the ability to dress properly, layer and shed properly so you don't end up perspiring in a cold-weather environment."

"You don't want to perspire in a cold-weather environment," Owens said. "That's very dangerous."

In subzero climates, profuse sweating can cause the body to lose heat quickly, inducing dangerous hypothermia.

The human body isn't the only thing that can become sluggish in the Arctic. Equipment does, too. Weapons and helicopters, for example, don't function the same in

A U.S. Army CH-47 Chinook helicopter drops off U.S. Air Force Airmen during training in Alaska. The exercise combined cold-weather skills, land navigation and Arctic movement training.

SENIOR AIRMAN PETER REFT/ U.S. AIR FORCE

subzero temperatures as they do in warmer climes. Arctic warfighting equipment is tested at the U.S. Army Cold Regions Test Center in Fort Greely, Alaska, and then assessed by Soldiers in USARAK. "We give them feedback on functionality, pitfalls, some improvements they could make," Owens said.

Soldiers assess weapons, skis, vapor-barrier boots, Canadian mukluks, which are high, soft boots traditionally worn in the Arctic, as well as communications equipment.

Keeping aircraft flying is no picnic. When gearing up an Apache helicopter at high altitudes, "it takes about six hours to spool up the electronics on it," Owens said. "Batteries have very little life when you are talking about cold weather. The oils, the hydraulics, are very sluggish."

Even when a Soldier is properly trained and equipped, using a weapon in the freezing cold can be a challenge. "Operating with Arctic mittens is very difficult," Owens said. "It's slow work."

The Soldiers learn how to layer and shed clothes properly, so they don't get frostbite — and to the other extreme — heat exhaustion. Those dangers require trained leaders to detect signs of trouble. "How do you identify when one of your Soldiers is suffering from the first signs of frostbite or heat exhaustion, believe it or not?" Owens said. "There are simple leadership tasks such as making your Soldiers drink water. At [minus 40 Celsius], nobody wants to drink water."

Half a world away, the challenges of military mountaineering in the Himalayas requires different kinds of equipment. Sometimes the latest technology isn't the best option. "There is limited, almost a nonexistence, of roads in the Nepalese mountains," Chhetri said. "You can't take your vehicle there."

Military operations — whether rescuing climbers from Mount Everest or fighting a decadelong Maoist insurgency that ended in 2006 — must be conducted, regardless of the harshness of the conditions. To get the job done, the Nepalese Army often travels by foot and relies on yak, sheep and mountain donkeys to move equipment, Chhetri said.

Few landing strips exist for fixed-wing aircraft, and in cold seasons, "you can't land there because of snow and ice," he said.

A U.S. Army paratrooper moves to a rally point after a successful airborne operation in Deadhorse, Alaska.
STAFF SGT. DANIEL LOVE/U.S. ARMY

VITAL COMPONENT

With a Stryker brigade combat team and an airborne brigade combat team, USARAK has deployed forces all over the world, including Afghanistan, Iraq and Kosovo. Cold-weather mountain warriors are essential in this global mission because cold regions represent 31 percent of the Earth's surface, and 27 percent of the world has mountainous terrain, Owens said.

Whether the mission is providing disaster relief, such as the devastating earthquake that plagued Nepal in 2015, killing nearly 9,000 people and injuring 22,000 — or combat missions in freezing temperatures — warriors who operate in high altitudes and cold weather must be some of the most physically fit on the planet.

In the case of USARAK, it helps that they live, work and even send their children to school in subzero temperatures, Owens said. It's part of everyday life.

"Our Soldiers not only train in cold regions, but they live there. Even in everyday activities, they know how not only to survive there but to thrive. Living in Alaska, especially in the Fairbanks area where our Stryker brigade combat team is located, it got to [minus 46 Celsius] in January. Those types of temperatures, you won't get anywhere else."

UNPREDICTABLE BEHAVIOR

Joint forces view multi-domain battle as key to future success

THE WATCH STAFF

Global proliferation of advanced military technology has eroded to some degree the advantage the U.S. and its military partners have held for decades, allowing adversaries to threaten use of the air, sea, land, space and cyberspace domains.

U.S. commanders and their allies and partners, however, envision a different battlefield. It's a battlefield where navies protect land forces and armies sink ships. It's a battlefield concept that invokes every operating domain potentially all at once.

The name for this technological and philosophical leap into 21st century warfighting is called multi-domain battle, and commanders see this increased agility as key to success in complex environments.

"I'd like to see the Army's land forces sink a ship, shoot down a missile and shoot down the aircraft that fired that missile," said U.S. Navy Adm. Harry B. Harris Jr., then commander of U.S. Pacific Command (USPACOM). "Components must increase their agility and provide support to each other across the warfighting domains."

Harris, who made the comments during the Association of the U.S. Army Institute of Land Warfare's Land Forces of the Pacific Symposium and Exposition (LANPAC) in May 2017, said the U.S., its allies and partners and even individual service components need to be more comfortable working in a "complex environment where our joint and combined forces are operating in each other's domains."

Multi-Domain Battle Overview

The goal of multi-domain battle is to enable the services to more effectively integrate capabilities across the air, sea, land, space, and cyberspace domains to deter and if necessary defeat highly capable potential adversaries. Enemies are posing unconventional threats — threats from cyberspace, electronic warfare and even unmanned aerial vehicles and improvised explosive devices.

If the technology and different military command structures are integrated, however, the U.S. and its partners could regain the advantage, Harris said. Many service-specific technological systems present a challenge to doing so. The systems often don't talk to each other, which hampers commanders' abilities to deliver ordnance to targets in a

U.S. Navy Adm. Harry B. Harris Jr., then commander of U.S. Pacific Command, says the United States will intensively focus its military training on multi-domain battle to better prepare forces for modern-day threats. REUTERS

timely fashion. The U.S. and its partners need to get "our alphabet soup of sensors and shooters talking to one another," Harris said. "Ideally, we'll get to a point where we'll see the joint force as a network of sensors and shooters, allowing the best capability from any single service to provide cross-domain fires."

That means the U.S. could detect a threat and Japan could eliminate it, or Australian sensors could detect a missile and relay the information to South Korea.

To test the concept, the U.S. Army of the Pacific (USARPAC) began sharpening these multi-domain capabilities with partners in the Indo-Pacific region at the Rim of the Pacific Exercise (RIMPAC) in 2018. RIMPAC is the world's largest international maritime warfare exercise and is held biennially off the coast of Honolulu, Hawaii.

In 2016, 26 nations, more than 40 ships and submarines, 200 aircraft and 25,000 personnel participated. In 2018, to test the multi-domain battle concept, U.S. and Japanese ground forces fired shore-based missiles to subdue a threat at sea.

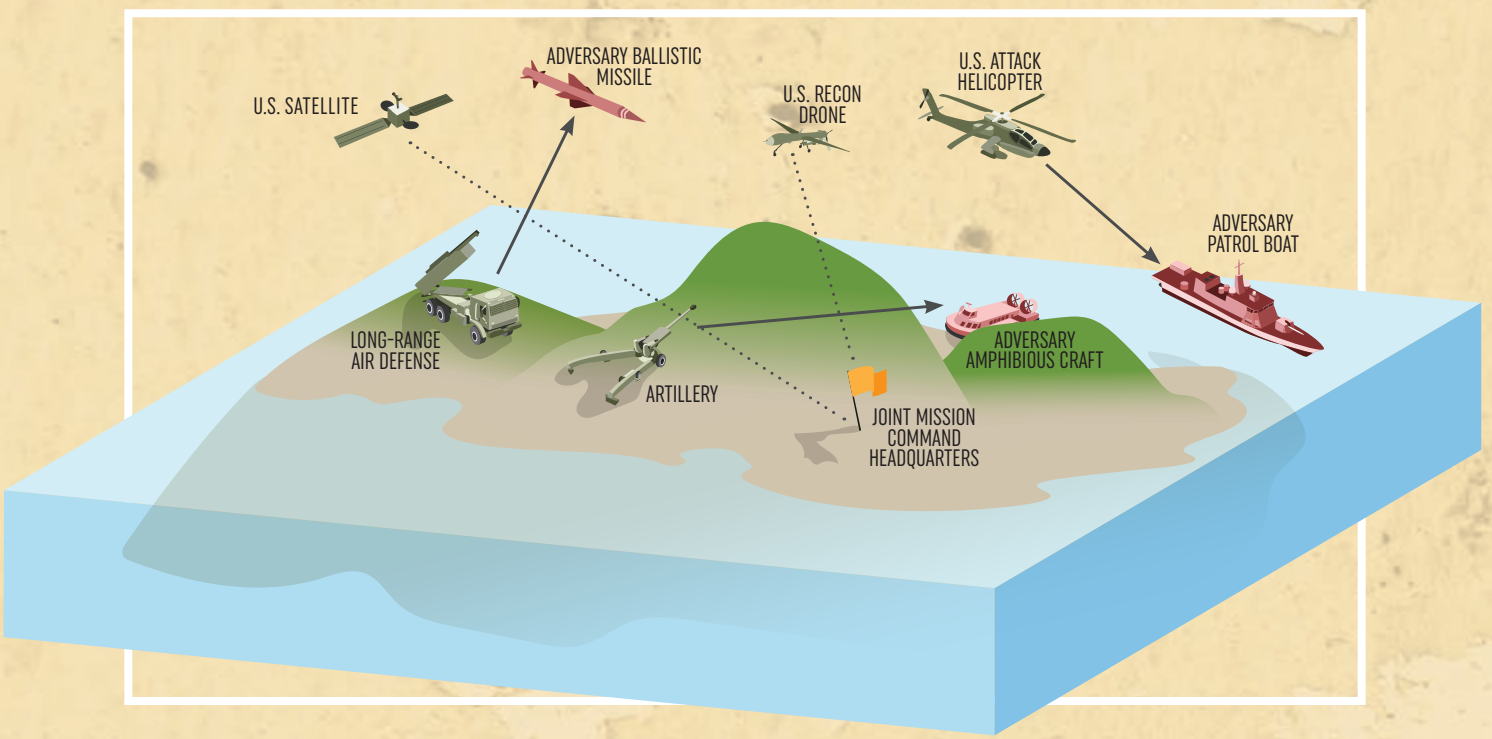
Gen. Toshiya Okabe, then chief of staff for the Japan Ground Self-Defense Force, said he looks forward to the day when the United States, Australia and other neighbors in the region implement the multi-domain battle concept. The interoperability it provides, he said, is essential to counter a potential adversary such as North Korea, which continues to defy United Nations sanctions related to its missile and nuclear weapons tests.

Multi-domain battle "must be very effective against North Korea," Okabe said during LANPAC 2017. He also pointed out that trilateral cooperation and multi-domain battle integration involving Japan, the Republic of Korea and the United States will be important to deter the secretive and bombastic North Korean regime.

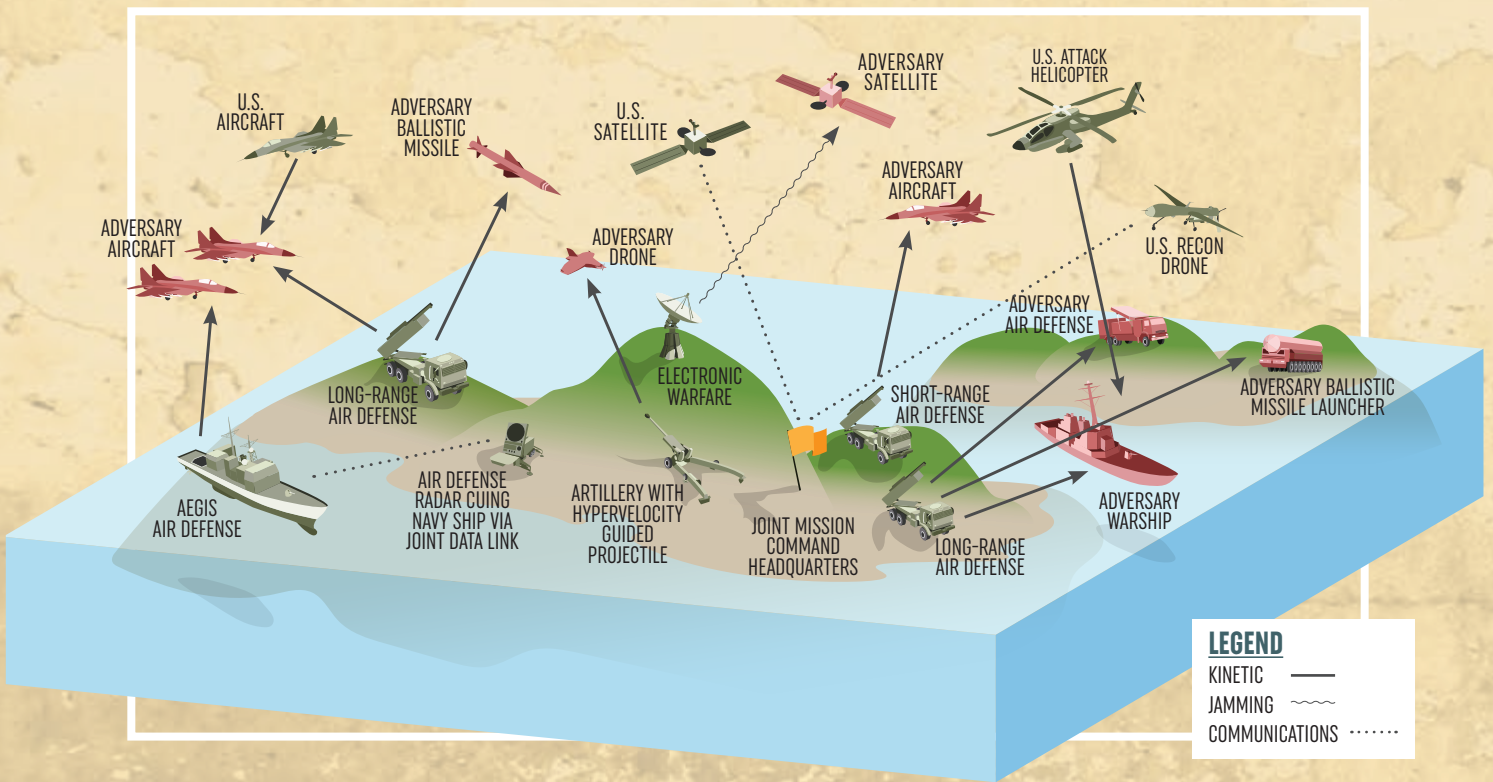
Okabe pledged to provide security cooperation with Japan's neighbors as well as the United States. "We will provide security cooperation to ASEAN [Association of Southeast Asian Nations] and to other countries in the region," Okabe said.

One of the keys to making those partnerships a success is to reduce the predictability of military operations, said Gen. David G. Perkins, then commander of the U.S. Training and Doctrine Command. If a problem arises in a domain — for example, a hostile ship poses a threat to U.S. forces — histori-

CURRENT CAPABILITIES



MULTI-DOMAIN BATTLE



The proliferation of advanced technology has eroded the advantage of the U.S. and its partners, allowing adversaries to threaten use of the air, sea, land, space and cyber domains. Multi-domain battle allows services to operate outside their conventional realms and adds a layer of flexibility and efficiency needed for 21st-century warfighting. *THE WATCH* ILLUSTRATION

Source: U.S. Army

cally, the U.S. Navy would have been asked to deal with it. "We tend to task that to the people who own it," Perkins said. The problem that creates, however, is that "if you only go after it with that domain, the enemy knows that."

Core Advantages

One of the key advantages of perfecting multi-domain battle is that it presents military leadership with multiple options to resolve a range of threats. It integrates the capabilities of different services and even militaries from other countries to defeat potential adversaries or rogue states, U.S. commanders say.

> "Ideally, we'll get to a point where we'll see the joint force as a network of sensors and shooters, allowing the best capability from any single service to provide cross-domain fires."
>
> **U.S. Adm. Harry B. Harris Jr., then** commander of U.S. Pacific Command

Not everyone has to bring skills from all domains to the table or invest financially to the degree that larger countries can, Perkins said. For example, one country might have a small Army but superior cyber skills, which could be used to allow joint forces to disrupt the military communications or navigation of an adversary.

One hypothetical example is a country that can defend its territorial waters, he added, but doesn't have a "blue water" Navy to project power abroad. Perhaps that country's contribution could be what the military calls A2AD, or anti-access/area denial. That country could defend its own territorial waters while agreeing to let the U.S. put military hardware in a militarily important geographic location to project power. "You don't have to do it all," Perkins said.

A2AD is a strategy that primarily uses land-based or shipborne cruise, ballistic and surface-to-air missiles to offset an opponent's capabilities. They are used to attack an enemy's critical ships, aircraft and ground sites. The progress that potential enemies have made across the globe in this arena have, in part, necessitated the move toward multi-domain battle and less predictable war plans, U.S. commanders say.

Regional Context

The rapidly growing economies, militaries and tensions in the Indo-Pacific necessitate the move toward a more sophisticated battle plan, wrote Gen. Robert B. Brown, commanding general of USARPAC, in an article on multi-domain battle.

The region contains 36 countries, more than half of the world's population, three of the world's largest economies and seven of the largest militaries. Dramatic technological shifts are occurring with unmanned vehicle capabilities, robotic learning, artificial intelligence and big data, which expand military competition between rivals, Brown said. Many of these new technological tools depend on the use of digital connectivity, making cyber defenses paramount.

Couple this with a region that is facing increasing security challenges, he said, and the need for multi-domain battle is obvious. The region wrestles with some of the world's most intractable challenges. North Korea flouts United Nations sanctions with its increasingly capable missile technology. China challenges international norms by militarizing the South China Sea, and Russia is active in the region with an increasingly provocative military posture, he said.

"The most dangerous threat in the Indo-Pacific comes from regional actors with nuclear arsenals and the intent to undermine the international order," Brown wrote. "Sophisticated denial capabilities and less-than-military forces managed by the state but backed by large militaries with interior lines of communication create the danger of faits accomplis."

Risk Taking

Battling unpredictable enemies requires culture change. Implementing the multi-domain battle concept across the Navy, Army, Marine Corps and Air Force will require intensive training and a culture change from the highest levels of the military, Harris said.

Technological upgrades must be made so threat detection and weapons systems can talk to each other — both among U.S. services and potentially with partner nations. "The joint force must have faster, longer-range, more precise, more lethal and importantly, cost-effective and resource-informed solutions," Harris said. "Not exquisite solutions that break the bank."

Speaking of the culture change that will be required in a universe where military services operate their own budgets and technological systems, Harris said: "I

Gen. Toshiya Okabe, former chief of staff of the Japan Ground Self-Defense Force, pledged security cooperation with his neighbors and allies and said he is excited about the prospect of countries in the region implementing multi-domain battle. STAFF SGT. DEBRALEE BEST/U.S. ARMY

look at our risk-averse culture and shake my head."

Changing that culture, he said, demands a sustained effort. "We must incorporate this concept into the way we train year-round," Harris said. "We all know that tomorrow's fights are won during today's training."

The Army, in its description of multi-domain battle, acknowledged the cultural and technological changes required. "Adm. Harris has asked the Army to sink ships, neutralize satellites, shoot down missiles, deny enemy command and control forces and restrict maritime movement. To support that goal, the Joint Force must fully integrate their sensors and weapons systems more than before. Collectively, we must become sensor agnostic and shooter agnostic."

Perkins said shared training and professional military education will be key in driving this interoperability between services and among friendly militaries. "When you train together, you work through problems," Perkins said. "Plus, you build relationships."

When discussing the more nimble and interoperable nature of tomorrow's military, Harris likened it to ride-sharing companies such as Uber and Lyft, which provide apps detailing specific services. "Instead of ride sharing," Harris said, "I'm looking for target sharing."

With more sophisticated enemies, he added, the stakes are high. "Our country must maintain credible combat power in concert with like-minded allies and partners to preserve the unimpeded access to all the global commons," Harris said. "Freedom, justice and a rules-based international order hang in the balance."

PREPARING FOR THE WORST

CBRN Response Force is always ready

THE WATCH Staff

It's a nightmare scenario: A 10-kiloton nuclear device is detonated at the entrance to New York City's Lincoln Tunnel. It could kill thousands, cause widespread panic and cut off much of the city from outside help.

The attack is almost unimaginable, but the job of the Defense CBRN Response Force (DCRF) is to imagine it and figure out how to save the most people and minimize the damage. Created in 1999, the DCRF is a national joint task force designed to respond to a catastrophic attack involving chemical, biological, radioactive or nuclear (CBRN) agents.

It has never been activated, but it undergoes training designed to mimic reality so that its members are prepared for the worst.

U.S. Army Maj. Gen. Richard J. Gallant, commander of the DCRF, calls it the nation's "insurance policy" against a major attack. "All of us hope nothing like this would ever happen, but we can't be caught unprepared if it did," Gallant told Federal News Radio. "We also have other capabilities. Because we're constantly training, we're also capable of responding to an all-hazards event."

Made up of 5,200 Soldiers, Sailors, Airmen and civilians from active-duty and reserve units, the DCRF is ready to deploy within 24 hours of being notified. The force includes people who specialize in chemical detection, search and rescue, decontamination, evacuation and much more. Its tasks fall into four general categories: aviation, logistics, medical and operations.

The scenario described was tested in Guardian Response 17, an exercise that simulated what a whole-of-nation response to a nuclear attack might look like.

For the exercise, nearly 4,100 Soldiers gathered at the Muscatatuck Urban Training Center in Indiana, which was made to appear as if it had suffered a bomb blast, complete with debris, smoke, downed trees and actors playing victims. Responders were asked to search for victims in the rubble, transport the wounded, and coordinate actions with local, state and federal officials. Most of the activity was done wearing cumbersome hazmat suits to prevent radiation exposure.

"We'll be treating between 60 and 80 casualties per hour," said U.S. Army Reserve 1st Lt. Erin Lovinus, a medical liaison officer with the 409th Area Support Medical Company. "We'll carry this mission on anywhere from 12 to 15 hours per iteration. This exercise is as realistic as it can be."

If a disaster hits the U.S. homeland, the DCRF will play a support role with local authorities in charge. Since all entities have different procedures, learning how to work together during an exercise like Guardian Response is key.

"It's much better to practice and improve response coordination," said Lt. Col. John Pitt, Muscatatuck Urban Training Center commander. "Practice that saves lives, eases suffering and provides assistance that helps return citizens' lives to normalcy."

A U.S. Army Soldier with the 51st Chemical Biological Radiological Nuclear Company of Fort Stewart, Georgia, escorts two civilian role players to a decontamination field site during Guardian Response 17.

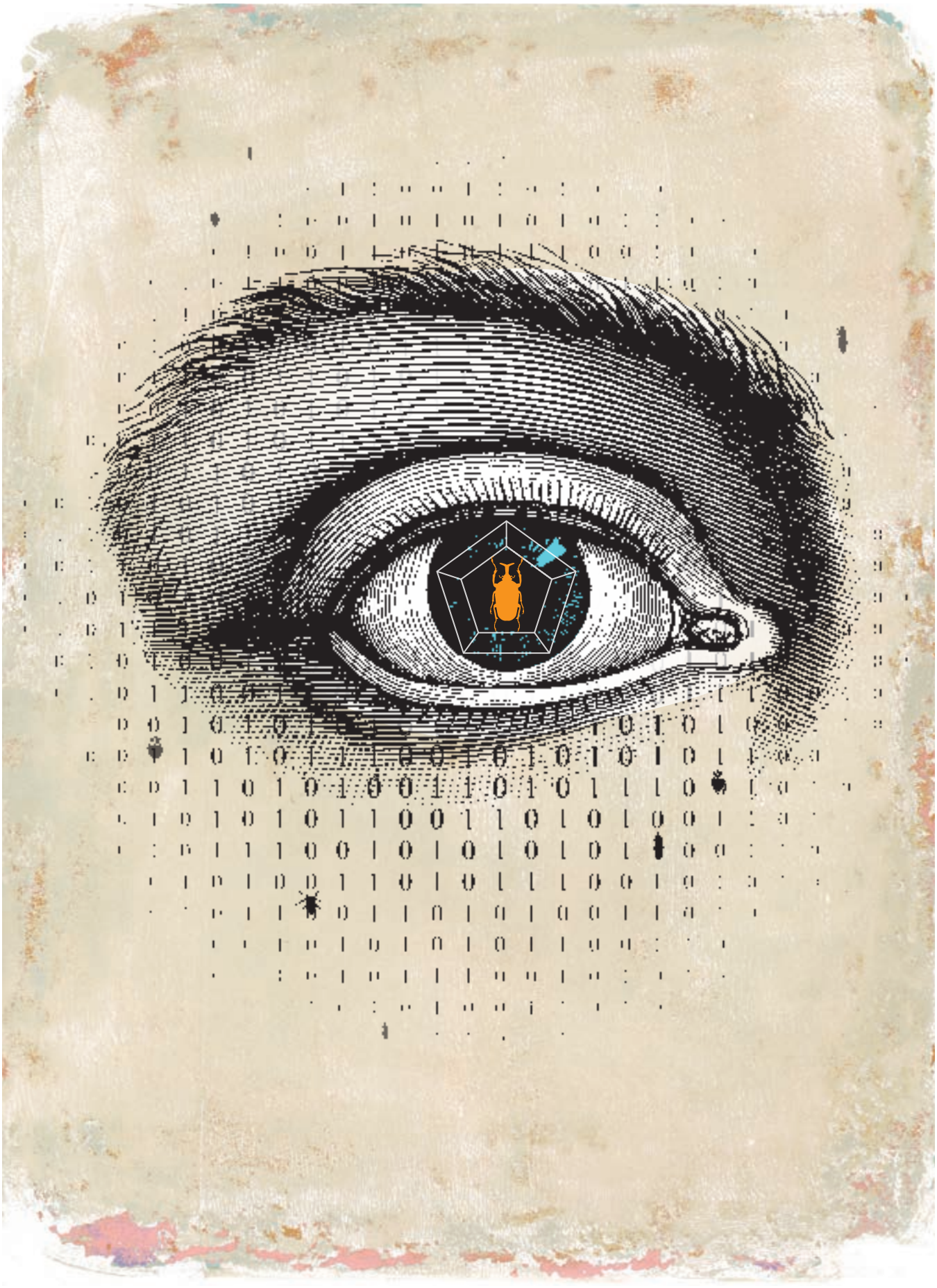
MASTER SGT. MICHEL SAURET/U.S. ARMY RESERVE

Each exercise tests the limits of DCRF capabilities and shows where the force must improve. For instance, Soldiers working in the "hot zone" must be rotated out every 90 minutes and spend time in the decontamination center. This constant rotation of personnel requires precise coordination achieved through repetition.

"We have to provide the right force with the right response and the right experience. If we use, God forbid, the worst possible scenario, then it helps us get after all those slower-developing scenarios that we respond to," Gallant said. "We are in support of the first responders, and we provide the capability that can augment their operations."

Soldiers prepare to treat victims during Guardian Response 17 at the Muscatatuck Urban Training Center in Indiana.

MASTER SGT. MICHEL SAURET/
U.S. ARMY RESERVE



A regional conference and friendly Pentagon cyber sleuths help bolster security

HACKING THE PENTAGON

THE WATCH STAFF

Safeguarding against cyber attacks is critical to the defense of any nation. Innovation is key as enemy tactics evolve and technological advances reveal new vulnerabilities. That's why the U.S. Department of Defense (DOD) launched the "Hack the Pentagon" program, a bold initiative to shore up cyber defenses.

Launched in 2016, the program was the first of its kind for the federal government. It empowers individuals to hunt for bugs and vulnerabilities in DOD websites available to the public.

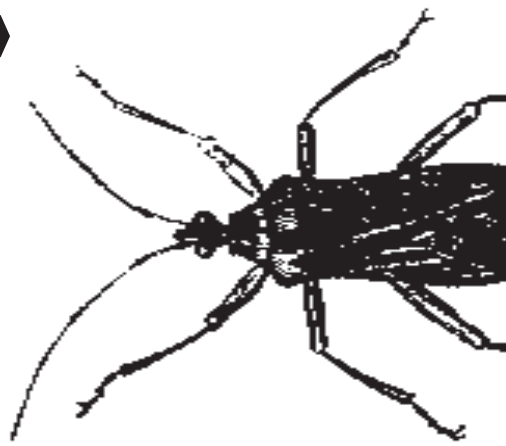
"We know that state-sponsored actors and black-hat hackers want to challenge and exploit our networks," then-U.S. Secretary of Defense Ash Carter said at the program's launch. "What we didn't fully appreciate before this pilot was how many white-hat hackers there are who want to make a difference, who want to help keep our people and our nation safer."

Managed by the DOD's digital service team, about 14,000 "hackers" registered to participate in the pilot program. They agreed to follow certain rules and in return were paid when finding legitimate vulnerabilities on DOD platforms. Websites such as Defense.gov, DoDlive.mil, DVIDSHUB.net (Defense Video Imagery Distribution System) and MyAFN.net (My American Forces Network Online) were among those chosen as targets.

"When it comes to information and technology, the defense establishment usually relies on closed systems," Carter said. "But the more friendly eyes we have on some of our systems and websites, the more gaps we can find, the more vulnerabilities we can fix, and the greater security we can provide to our warfighters."

The first vulnerability report was filed just 13 minutes after the pilot launched, and within six hours, there were 200 reports. A total of $75,000 was paid for reports submitted over a month.

One of the hackers — a high school student — said he was thankful for the unique opportunity. "It was a great experience," David Dworken said. "I just started doing more and more of these bug bounty programs and found it rewarding — both the monetary part of it and doing something that is good and beneficial to protect data online in general."



The program was considered a huge success. Hundreds of vulnerabilities were discovered that had been missed by government teams, including more than a dozen considered high risk, said Kate Charlot, principal director for cyber policy within the U.S. Office of the Secretary of Defense. She shared the program with cyber security leaders and experts from the Middle East during the U.S. Central Command's (CENTCOM's) Central Region Communications Conference (CRCC) in April 2017 in Alexandria, Virginia, in the United States. The U.S. Army is planning a similar program.

The DOD has also created a procedure for people to report vulnerabilities on any DOD public site. Like the bug bounty program, it's the first of its kind for the U.S. federal government, basically the equivalent of a digital "see something, say something," campaign.

U.S. Army Maj. Gen. Mitchell Kilgo, director of Command, Control, Communications and Computer Systems at U.S. Central Command, left, speaks with his counterpart from Saudi Arabia, Maj. Gen. Riyadh bin Abdul Aziz Al-Dugheither, at a 2017 cyber conference.

COL. LEERNEST M. RUFFIN/U.S. AIR FORCE

INCREASING VULNERABILITIES

The need for these programs is growing exponentially. Children's toys, refrigerators, home security alarms and traffic lights are just a few of the abundant internet-enabled devices present in our daily lives. While each new item offers convenience and innovation to people across the world, there is a trade-off: Web-based systems and products are vulnerable to hacking. Air-conditioning systems that cool the rooms storing government computer servers can be interrupted, causing network disturbances. A doll that records voices to entertain and comfort children can record private conversations inside homes. As technology advances, the number of potential vulnerabilities also grows, increasing the importance of preparing for cyber breaches.

Creating opportunities for military, academic, government and industry experts to collaborate and gain new perspectives on each other's roles in national security is imperative to address these challenges. The CRCC was one of these opportunities; it focused on cyber incident response. The relationships developed during the conference enable organizations to recover more quickly and with less damage when an incident occurs.

"I believe our best defense is to be proactive," then-CENTCOM Deputy Commander Lt. Gen. Charles Brown Jr. said during the CRCC conference, attended by representatives from Bahrain, Egypt, Iraq, Jordan, Kuwait, Lebanon, Oman, Qatar, Saudi Arabia, the United Arab Emirates and the U.S. He explained that each country is stronger by collaborating with various organizations within a country and with cyber experts across the world.

To do this requires dismantling a culture of "information silos" that exists in many organizations. This will help leaders make decisions based on all available information, explained U.S. Army Maj. Gen. Mitchell Kilgo, director of CENTCOM's Command, Control, Communications and Computer Systems. "You must understand your critical assets and their associated vulnerabilities," Kilgo said. "You must talk about the risk to the mission and the risk to critical assets. This is important for commanders."

Representatives from private companies and academia gave presentations at the conference. Senior government representatives spoke about the best practices in their countries, providing insights into topics worthy of future discussions.

"In Iraq, the growth of the internet's popularity — for security, business and personal use — coincided with a lack of secure cyber infrastructure," explained Maj. Gen. Mahdi Yasir Zubaidi, director of military communication for Iraq's Ministry of Defense. "This raised awareness of the need to understand the dangers of cyber crimes accompanying every new technological development, especially in the context of society's transformation into a cyber community."

Experts said a good cyber defense takes more than just software. To better protect networks and identify vulnerabilities, system administrators must be trained to understand how adversaries think and how to "hunt" them down in a network.

Countries such as Kuwait have had success in developing a whole-of-government approach to cyber security. Mohammad Altura, executive board member of Kuwait's Communication and Information Technology Regulatory Authority, gave a detailed presentation about his country's strategy development process. Kuwait has identified objectives to focus

THE WORLD'S
TOP 10
in Cyber Security

The Global Cyber Security Index (GCI) 2017 shows that commitment to cyber security is not tied to geographic location. Three of the countries ranked in the Top 10 are from the Indo-Pacific, two are from Europe and two are from North America. The other three are from Africa, the Arabian Peninsula and the Caucasus.

1 Singapore
2 United States
3 Malaysia
4 Oman
5 Estonia
6 Mauritius
7 Australia
8 Georgia
9 France
10 Canada

Source: International Telecommunication Union

on over the next three years. The three principle strategic initiatives are to promote a culture of cyber security in Kuwait; to safeguard and continually maintain the security of national assets including critical infrastructure, information, communication technologies and the internet; and to promote cooperation, coordination and information exchange with local and international bodies in the field of cyber security.

Kuwait has numerous projects planned for implementation over the next few years that will help the country achieve its goals, such as establishing a Kuwait National Cybersecurity Center and establishing a national threat intelligence team that can work with global organizations to help identify the threats to Kuwait.

"There is an absence of international laws regarding cyber security today," Altura said. "With military, the laws are very clear regarding a country's sovereignty. With cyber, it's still open."

Dr. Ghazi Salem Al-Jobor, chairman of the board of commissioners and CEO of Jordan's Telecommunications Regulatory Commission, said the conference gives Jordan's government and military a greater awareness of the importance of collaborating with the private sector and regional partners when implementing cyber security.

Al-Jobor said: "Learning from the United States' experience and others' experiences and measures was very useful in steering our thoughts on how to mitigate cyber attacks and the importance of the factors that need to be taken into account to have effective national and regional response measures."

Thanks to the regional conference and the internal DOD hacking program, governments are better equipped to protect against devastating cyber attacks.

> "I believe our best defense is to be proactive."
>
> CENTCOM Deputy Commander
> Lt. Gen. Charles Brown Jr.

NORAD THE BEGINNING

Brian D. Laslie, Ph.D.

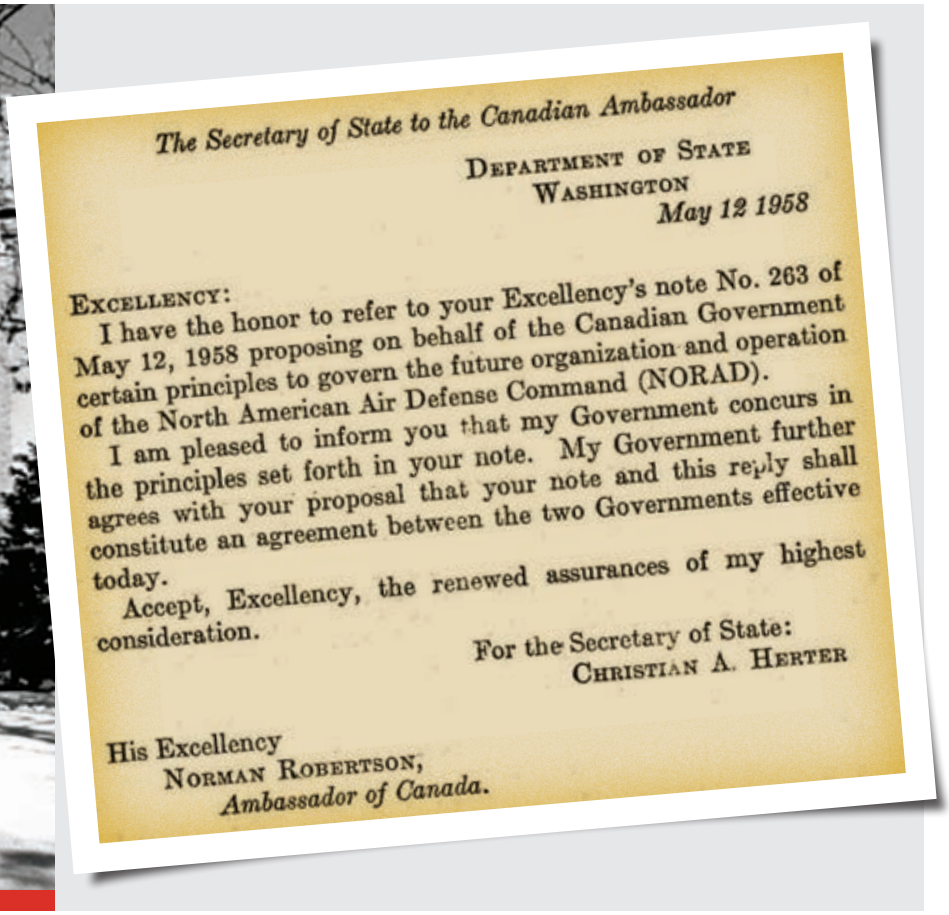
It is always treacherous to ask a historian when an event began or ended. "It depends" will likely be the answer. Take, for example, the beginning of World War II. Americans might use the date December 7, 1941. Many in Europe would say September 1, 1939, or even January 30, 1933, when Adolf Hitler became chancellor of Germany. Again, "it depends" largely on where and when an event began for "us."

The same is true for the North American Aerospace Defense Command (NORAD). NORAD's official birthday is May 12, 1958, the date the United States and Canada exchanged diplomatic notes and officially created NORAD. The truth is that NORAD had already been protecting the two countries and was conducting this mission for eight months when the two leaders signed the agreement.

The post-World War II environment and the rise of the Cold War dictated a united defense between Canada and the United States to protect both nations against a possible attack from the Soviet Union. While the United States had the lion's share of offensive capability, Canada's vast northern regions provided the means to detect and respond effectively against an incoming attack. Neither country had the ability to defend against an attack alone.

By 1957, the details had been worked out, and the top defense officials in each nation approved the formation of the "North American Air Defense Command." Canada and the United States announced in August that year that the two nations planned to cooperate on air defense. The military wasted no time in making this proposed cooperation an operational reality. Official operations began on September 12, 1957, at Ent Air Force Base in Colorado Springs, Colorado, after U.S. Air Force Gen. Earle Partridge, commander of the Continental Air Defense Command (CONAD), issued the stand-up order. Partridge's message read: "Announcement is made of the establishment of the North American Air Defense Command … effective 12 September 1957 as a Combined Command for the air defense of the continental United States, Canada, Alaska and the Northeast Area." The date is historically significant. As Joseph Jockel, author of Canada in NORAD, 1957-2007: a History said: "NORAD became what its prime creators in the United States Air Force (USAF) and Royal Canadian Air Force (RCAF) originally wanted it to be: namely, just a practical and useful continental air defense headquarters."

Ent provided the ideal location. Already the home of CONAD and its subordinates, including USAF Air Defense Command (ADC), the base was situated near the center of the country. Partridge, who was already the ADC and CONAD



The Secretary of State to the Canadian Ambassador

DEPARTMENT OF STATE
WASHINGTON
May 12 1958

EXCELLENCY:

I have the honor to refer to your Excellency's note No. 263 of May 12, 1958 proposing on behalf of the Canadian Government certain principles to govern the future organization and operation of the North American Air Defense Command (NORAD).

I am pleased to inform you that my Government concurs in the principles set forth in your note. My Government further agrees with your proposal that your note and this reply shall constitute an agreement between the two Governments effective today.

Accept, Excellency, the renewed assurances of my highest consideration.

For the Secretary of State:
CHRISTIAN A. HERTER

His Excellency
NORMAN ROBERTSON,
Ambassador of Canada.

commander, also became the first commander in chief of NORAD, and the senior Canadian RCAF official, Air Marshal Roy Slemon, who had been the key Canadian delegate in most of the cooperation talks, became deputy commander.

Partridge enlisted in the U.S. Army at age 17 during World War I, serving in Europe and at the Battles of Meuse-Argonne and Saint-Mihiel before returning home and attending West Point. He earned his wings and went on to attend and instruct at the Air Corps Tactical School prior to World War II. He eventually served as the deputy commander of the 8th Air Force in 1944 during World War II. He later served as commander of the 5th Air Force during the Korean War and as the commander for the famed Far East Air Force, making him one of the few Air Force officers to have served in all three conflicts. He was one of the cadre of air power practitioners who came of age in the interwar years and applied this knowledge in World War II.

Slemon, the first Canadian deputy of NORAD, joined the Royal Canadian Air Force in 1922. During World War II, Slemon was a senior staff officer of the No. 6 Bomber Group and ended the war as deputy air officer commander in chief of the RCAF Overseas. After the war, he went on to be air officer commanding Training Command. When he became deputy commander of NORAD in 1957, he was the only member of the RCAF's "originals" still serving on active duty. Much of his early flying career included years mapping the vast reaches of the Canadian North and the sub-Arctic. Few men could say they understood the North as Slemon did.

These two officers, Slemon and Partridge, represented the perfect pairing to head the Air Defense Command and ensure the safety of the two countries in subsequent years.

Eight months after operational establishment of the command, on May 12, 1958, the two nations announced they had formalized the cooperative air defense arrangement as a government-to-government binational defense agreement that became known as the NORAD agreement. That is why the May 12 date represents the official NORAD birthday as opposed to the September 12 date, which represents more the innovative spirit and "can do" attitude that both militaries often apply to problem solving.

NORAD operations began in 1957 at Ent Air Force Base in Colorado Springs, Colorado.

The governments of Canada and the United States made the establishment of NORAD official on May 12, 1958.

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

NORAD: 60 AND GOING STRONG

In the next issue of *The Watch*, catch our complete coverage of the North American Aerospace Defense Command's 60th anniversary. The magazine will showcase anniversary events in Colorado and Canada as NORAD celebrates its past, honors the uniqueness of the binational command and looks to the future as the command evolves to meet ever-changing threats.