

THE WATCH



v2

TRUSTED FRIENDS
SEEING VALUE IN DEFENSE PACTS

HIGHEST PRIORITY
ENHANCING MISSILE DEFENSE

SPACE DEBRIS
COPING WITH DANGEROUS OBJECTS

CONTENTS

THE WATCH // **COLLABORATIVE DEFENSE**



Revisionist powers Russia and China have changed global strategic dynamics by fielding advanced long-range weapons systems and engaging in increasingly aggressive efforts to expand their global presence and influence, including in the approaches to the United States and Canada. Our competitors currently hold our citizens and national interests at risk, and we must anticipate attacks against our defense and civilian infrastructure in the event of a conflict. As a result, it is clear that the homeland is no longer a sanctuary.”

— **GEN. TERRENCE J. O'SHAUGHNESSY**

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



Features

From *The Watch* Staff **04**

DEPARTMENTS

Impressions **05**

Key Leader **18**

Health Watch **28**

Flashback **38**

World View **46**

Innovation **58**

Rapid Response **64**



06

Sky-High Safety Net

NORAD identifies threats, enforces air restrictions.

12

First Lines of Defense

Military, intelligence collaboration protects homelands worldwide.

22

The Highest Priority

A vigorous missile defense strategy is essential to security at home and abroad.

32

Space Waste

Working together to defend the planet from orbiting debris.

40

Powerful Plans

Energy generation, resilience are key challenges for military logisticians.

48

Defending Cyberspace

NATO countries simulate cyber attacks to boost capabilities.

52

Perfecting the Kill Chain

New technology links sensors, shooters to speed military response.

60

On Target With Missile Defense

Test of next-generation integrated air and missile defense system successful.

ABOUT THE COVER

This illustration by *The Watch* depicts the critical role air power plays in homeland defense. The North American Aerospace Defense Command deploys fighter jets to protect air approaches, critical infrastructure and major events.

DEAR READERS,

Welcome to the second edition of *The Watch*, a homeland defense magazine published by U.S. Northern Command. In this edition, we highlight the value of local, regional and international defense partnerships. From the Five Eyes alliance involving Australia, Canada, New Zealand, the United Kingdom and the United States to trilateral patrols in Southeast Asia, military partnerships and intelligence-sharing pacts are cornerstones of homeland defense. They have uncovered spy rings, led to the apprehension of suspected terrorists and allowed friendly nations to help each other stay safe.

For these alliances to succeed, defense partners must embrace emerging technology to counter increasingly sophisticated threats. One article details how the U.S. military is testing new technology that speeds up its response to a cruise missile threat. The Advanced Battle Management System leverages artificial intelligence and machine learning to more seamlessly produce a coordinated response to a cruise missile attack.

We also explore the changing nature of homeland defense. In our key leader profile, Brig. Gen. Pete M. Fesler, deputy director of operations for the North American Aerospace Defense Command (NORAD), examines how the U.S. and its partners are investing in cutting-edge technology to meet new threats. Potential adversaries are fielding systems that would allow them to conduct conventional strikes against the U.S. homeland, Fesler explained, requiring the U.S. and its partners to be capable of conducting joint and combined operations in all domains.

All of these homeland defense efforts require sound military logistics, so this edition explores the science of getting military cargo and personnel to the fight in a technologically sophisticated environment. As military strategists throughout history have concluded, logistics success often makes the difference on the battlefield.

The battlefields of today include the crowded landscape of space, where scientists are tracking 8,800 metric tons of debris orbiting Earth. Although space junk threatens satellites and the International Space Station, the challenge of neutralizing it is stimulating partner nations to discover scientific solutions.

Finally, *The Watch* devotes part of this edition to the history and mission of NORAD, a partnership between Canada and the United States that has protected North America since the beginning of the Cold War. From patrolling the skies over major events to intercepting military aircraft as they approach North America, NORAD aviators defend the homeland every day.

We hope *The Watch* continues to spark dialogue about homeland defense, and we invite you to contact us at n-nc.peterson.nncj3.mbx.the-watch@mail.mil with your perspectives.

Regards, *THE WATCH* STAFF



THE WATCH

Homeland Defense

Volume 2 2020

USNORTHCOM LEADERSHIP

TERRENCE J. O'SHAUGHNESSY
General, USAF
Commander

WILLIAM J. DUMONT
Vice Admiral, USN
Deputy Commander

AUSTIN E. RENFORTH
BRIGADIER GENERAL, USMC
Acting Chief of Staff

CONTACT US

THE WATCH

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

email:

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

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

ISSN 2577-0098 (print)



The U.S. carried out an intercept test of the Terminal High Altitude Area Defense (THAAD) system in August 2019. The THAAD interceptor was launched from the Marshall Islands and was the first test using a remote launcher kit. It was the 16th successful test of the THAAD system since 2005.

U.S. MISSILE DEFENSE AGENCY





SKY-HIGH SAFETY NET

THE WATCH STAFF

NORAD identifies threats, enforces air restrictions

They patrol the skies over the biggest events — Super Bowls, World Series games and rocket launches. More frequently, they intercept pilots who violate flight restrictions by flying over protected areas such as the nation’s capital or the presidential retreat.

Aviators from the North American Aerospace Defense Command (NORAD) defend the homeland every day by identifying threats and interacting with civilian and military pilots. The events that often make headlines, however, are NORAD’s military-to-military encounters, such as when NORAD pilots intercept long-range Russian bombers.

NORAD is charged with the critical missions of conducting aerospace warning, aerospace control and maritime warning to defend North America. Since the terrorist attacks of September 11, 2001, NORAD aircraft have conducted more than 2,000 intercepts of nonmilitary aircraft over North America under Operation Noble Eagle, said Steven Armstrong, NORAD’s strategic engagement chief and vice director of operations. “Since 9/11, NORAD, through Operation Noble Eagle, has had a no-fail mission to be able to find, track and identify any suspect aircraft inside North America that could do us harm,” Armstrong told *The Watch*. “We’ve found over the years the best way to assess potential intent is by putting eyes inside the cockpit of the suspect track. That is why intercepting



NORAD enforces temporary flight restrictions over major events, such as Super Bowl LII in Minneapolis, Minnesota.

AFP/GETTY IMAGES

sovereignty missions in North America. Aircraft used to carry out the mission include F-15, F-16, F-22 and CF-18 fighters, U.S. Coast Guard MH-65 Dolphin helicopters, airborne warning and control systems (AWACS), and air refuelers.

When a single-engine aircraft entered restricted airspace near President Donald Trump's Mar-a-Lago retreat on April 20, 2019, and failed to communicate with air traffic controllers, an F-16 fighter and military helicopter intercepted it, according to a statement released by NORAD. Upon intercept, the pilot established communications and left the restricted airspace. When the president visits his Florida retreat, all air operations — with few exceptions — are prohibited within a 16-kilometer circle around Palm Beach International Airport.

While those intercepts gain local notice, NORAD intercepts of Russian aircraft make international news. In March 2020, U.S. and Canadian aircraft intercepted two Russian turboprops that flew over the Beaufort Sea near Alaska. The Russian Tu-142 maritime reconnaissance aircraft were escorted by F-22 and CF-18 planes, NORAD said in a news release. The Russian planes never left international airspace during the duration of the four-hour flight but flew within about 80 kilometers of

the aircraft with either fighters or helicopters is essential in assessing hostile intent before a hostile act can be committed.”

Operation Noble Eagle was the name given to the military response to the terrorist attacks, and it now applies to all air sov-

Alaska's coast.

“NORAD's top priority is defending Canada and the United States,” NORAD Commander Gen. Terrence J. O'Shaughnessy said in a statement following a 2019 intercept of Russian aircraft. “Whether responding to violators of restricted airspace domestically or identifying and intercepting foreign military aircraft, NORAD is on alert 24 hours a day, seven days a week, 365 days a year.”

The joint U.S.-Canadian Air Defense Identification Zone (ADIZ) extends 322 kilometers from the coastline in most areas and is primarily over water. It serves as a national defense boundary for aerial incursions. Any pilot who wants to fly in or through the boundary must file a defense visual flight rules plan or an instrument flight rules plan beforehand.

Aircraft approaching and crossing the North American ADIZ must have an operational radar transponder and maintain two-way radio contact. Aircraft flying in the zone without authorization may be treated as an enemy aircraft, which could lead to interception by fighter jets.

It's not uncommon for Russian military pilots to fly into the North American ADIZ, according to NORAD's Armstrong. Since Russia resumed long-range aviation activity in 2007, he said, NORAD has averaged about seven intercepts of Russian military aircraft per year. “These numbers have varied each year from as high as 15 to as low as zero,” he said.

NORAD is a binational command of Canada and the U.S., so air intercepts are conducted with resources from both countries. Most intercepts, however, occur over the U.S., Armstrong said.



Florida Air National Guard F-15s from the 125th Fighter Wing, Jacksonville, Florida, defend the skies over the Kennedy Space Center during the first manned space launch in nearly nine years. The SpaceX Falcon 9 rocket took off for the International Space Station in May 2020. The F-15s were operating under the North American Aerospace Defense Command (NORAD).

NORAD

“Whether responding to violators of restricted airspace domestically or identifying and intercepting foreign military aircraft, NORAD is on alert 24 hours a day, seven days a week, 365 days a year.”

– Gen. Terrence J. O’Shaughnessy, commander of the North American Aerospace Defense Command and U.S. Northern Command



The White House is in a Special Flight Rules Area that is closely guarded by NORAD.

THE ASSOCIATED PRESS

Two F-16 Fighting Falcons begin rolling into position for a rapid descent during a training mission over San Francisco Bay.

MASTER SGT. LANCE CHEUNG/U.S. AIR FORCE



RADIO SILENCE CAN TRIGGER INTERCEPT

NORAD will conduct intercepts over the homeland if an aircraft enters a Special Flight Rules Area around the nation's capital or another temporary flight restrictions (TFR) area, Armstrong said. TFRs are established on any given day due to the movement of top government officials, special events, natural disasters or other unusual events. They are established by the Federal Aviation Administration (FAA) and enforced by NORAD where appropriate.

If an aircraft enters restricted airspace and is unresponsive to the FAA, NORAD may scramble fighters or rotary wing aircraft to conduct an intercept. NORAD uses several methods to notify pilots to leave an area immediately. "Some of the methods used to communicate with pilots include radio contact, visual hand signals, rocking of wings and release of flares to signal the aircraft they have entered restricted airspace," Armstrong said.

An intercept typically means that NORAD aircraft flew alongside, identified and then escorted the civilian aircraft out of restricted airspace, Armstrong said. The civilian aircraft is often led to a nearby airport and met by local law enforcement for further investigation.

NORAD has air resources in multiple locations, so it can quickly access all parts of Canada and the U.S. "There's a great deal of coordination that takes place as NORAD analyzes potential threats and intelligence information, decides where to position alert aircraft and determines readiness levels for an effective air defense posture," Armstrong said.

SOUTHERN PARTNERS

NORAD also keeps watch on the U.S. southern border. The command has a long-running partnership with Mexico's National Defense Forces (SEDENA) to track

suspicious flights that cross the U.S.-Mexico border. Each year, SEDENA, NORAD and U.S. Northern Command (USNORTHCOM) conduct exercise Amalgam Eagle to practice mutual warning and information sharing to produce a cooperative response to illicit flights that cross the border.

Such exercises "serve to expand and enhance our trusted relationships with our partners and friends in all levels of the Mexican government," said Joseph Bonnet, director of Joint Training and Exercises for NORAD and USNORTHCOM.

Amalgam Eagle includes command post and field training exercises to enhance airspace control procedures with support from civilian agencies from both countries.

The exercise consists of two phases. The first involves practicing procedures for the handover of a derelict aircraft — a term used when an aircraft is not under human control. The second phase focuses on national procedures for monitoring an illegal flight and the cooperative hand-off of the aircraft from one nation to the other.

The objectives are to maintain operational and communications capabilities among NORAD, USNORTHCOM and SEDENA; to build a common operational picture of the continental air domain; and to continue developing and using communications protocols regarding illicit aircraft traveling through U.S.-Mexico airspace.

The exercises over the past several years "have grown in scope and complexity, and have mutually benefited our military forces in building capacity and capabilities," Bonnet said. "Today, the Mexican and U.S. militaries enjoy outstanding collaborative relationships based on trust and confidence, which are critically important to future cooperation and mutual support in response to a crisis such as an illicit flight that crosses the U.S.-Mexico border."

FIRST LINES OF DEFENSE

**Military, intelligence
collaboration protects
homelands worldwide**

THE WATCH STAFF

Military and intelligence-sharing cooperation agreements play prominent roles in the history of homeland defense. Friendly governments collaborated to uncover a Soviet spy ring stealing nuclear secrets. A regional defense pact led to the capture of terrorist kidnappers in Southeast Asia. More recently, Indian insurgent groups operating inside Bangladesh were disbanded, thanks to military coordination between neighboring border forces.

In a digital world where threats can originate from any point on the globe, like-minded countries are coming to an important conclusion: Homeland defense starts with the efforts of friendly nations far from home. “There are folks out there in the world, countries out there in the world who do not share our values and our approach to freedoms and mostly the rules-based order,” Canadian Prime Minister Justin Trudeau said after a meeting with Commonwealth partners Australia, New Zealand and the United Kingdom, according to The Canadian Press. “So, the importance of like-minded friends and partners

like us four to stand together ... provides a response and a solidarity that is a clear message to those around the world who do not play by the same rules.”

FIVE EYES WATCH THE WORLD

At a time when the Islamic State of Iraq and Syria (ISIS) recruits online and plans attacks worldwide, intelligence sharing has become an indispensable part of the anti-terror arsenal. Terror plots and international cyber attacks draw the attention of what many experts say is the world’s most significant intelligence-sharing entity — the Five Eyes alliance.

Born out of a fight for survival during World War II, the alliance started with intelligence cooperation between the United Kingdom and the United States. The countries forged a close intelligence relationship that later was expanded to include Canada, Australia and New Zealand. The name of the alliance comes from the number of countries that have access to “Eyes Only” information. The intelligence sharing melds technologically sophisticated systems from



the U.S. with the U.K.'s more traditional human intelligence operations, which are strong in the former Soviet Union, Europe and the Middle East, according to Reuters.

The relationship between the U.K. and the U.S. was formalized in 1946. A galvanizing event was a joint effort to decrypt Soviet intercepts that helped reveal that spies had compromised the U.S. Manhattan Project. "There was in the United States a creeping realization that maybe the Russians weren't going to be their friends in the 1950s," said Kristian Gustafson, senior lecturer of intelligence studies at Brunel University London, according to CNN.



Julius and Ethel Rosenberg were convicted of passing atomic secrets to the Soviets after a collaborative effort by the United States and the United Kingdom deciphered Soviet codes and uncovered a spy ring.

THE ASSOCIATED PRESS

The intelligence breakthrough that revealed the espionage occurred in 1946 when the U.S. and U.K. deciphered the code Moscow was using to send telegraphs, according to an account by the Smithsonian Institution. Venona, the name given to the decoding project, remained an official secret until it was declassified in 1995.

As decryption processes became more sophisticated, the allies discovered several spies. Investigations resulted in the execution or imprisonment of a dozen people who had passed atomic secrets to the Soviets.

As the value of this intelligence pact became apparent, the circle of trusted partners grew. Canada was brought into the fold in 1948, followed by Australia and New Zealand in 1956. The alliance was vital during postwar World War II tensions with the Soviets. "The cooperation was crucial for both countries during the Cold War," an analysis by the UK Defence Journal website stated. "For Britain, an example was the Five Eyes role in providing complementary intelligence for tracking Soviet submarines with ballistic missiles in the North Atlantic and the North Sea, and for the United States, it relied on long-established British listening posts in territories that were part of Britain's empire for signals of intelligence, especially in the Middle East."

More recently, the Five Eyes alliance has been focusing on terrorist movements, cyber warfare and the situation on the ground in war-torn Syria, according to media reports. After the November 2015 terror attacks in Paris, for example, Five Eyes shared with France some of its most sensitive intelligence on ISIS in Syria.

Intelligence-sharing agreements also have been struck within the North Atlantic Treaty Organization (NATO), which has existed since 1949. Since that time, NATO has grown from an alliance of 12 nations to 29. NATO grew largely out of Cold War fears of Soviet aggression after the Soviet blockade of Berlin and a communist coup in Czechoslovakia. Belgium, Canada, Denmark, France, Iceland, Italy, Luxemburg, the Netherlands, Norway, Portugal, the U.K. and the United States signed the initial treaty on April 4, 1949. After the Soviets detonated an atomic bomb in 1949 and the Korean War started in 1950, NATO members established a central headquarters and committed to providing joint military resources to address threats.

A key provision of the NATO treaty, Article 5, states that if one member of the alliance is attacked in Europe or North America, it is considered an attack on them all. That put Western Europe under the nuclear umbrella of the United States. The only time NATO's mutual defense provision has been invoked, however, was to support the U.S. after the September 11, 2001, terror attacks on New York and Washington. The alliance activated reconnaissance flights over the U.S., and NATO participated in the U.S.-led military operations in Afghanistan.

REGIONAL RESPONSE

Thousands of kilometers away, Indonesia, Malaysia and the Philippines were struggling with a shared problem. Local terror groups were using the channels and inlets along their coastlines to move people, cash and weapons around remote islands to launch terror attacks and kidnappings. The nations decided to pool resources, and in July 2017 they launched trilateral naval and aerial patrols to deter ISIS-inspired terrorists.

Called Indomalphi — a combination of the names of Indonesia, Malaysia and the Philippines — the partnership established maritime command centers in each nation. The creation of the patrols marked "a concrete step taken by the three countries" to maintain "stability in the region in the face of non-traditional real threats such as piracy, kidnapping, terrorism and other transnational crimes in regional waters," according to a statement released by the governments.

The collaboration paid dividends immediately. Brig. Gen. Custodio Parcon, commander of Indomalphi, confirmed that two suspected terrorists affiliated with the ISIS-inspired Abu Sayyaf Group were arrested in the Philippines just days after the defense partnership was announced. The suspects — Ara Samindi and Omar Harun — were wanted



Soldiers from many nations march during the opening ceremony of the 2018 summit of the North Atlantic Treaty Organization in Brussels, Belgium.

AFP/GETTY IMAGES

by Malaysia and accused of kidnappings off the coasts of Malaysia and the Philippines.

Then-Malaysian Defense Minister Datuk Seri Hishammuddin Hussein said the partnership is broader than coordinated patrols, however. It includes regular intel-

ligence sharing, and the counterterrorism efforts now include police forces. “It is the first collaboration involving all three countries which combines military and police efforts on intelligence-sharing,” he said, according to a report in the *New Straits Times* newspaper. “The approach is timely and able to bring a positive impact on efforts to address the threat of violence in Southeast Asia.”

Operating procedures for maritime patrols allow military personnel to enter a partner country’s waters during the hot pursuit of suspected criminals. The countries also agreed to establish transit corridors for commercial activities. Due to the urgency of the terrorist threat, the cooperation was achieved “despite territorial disputes and overlapping exclusive economic zones,” stated an article by Asia Pacific Pathways to Progress Foundation




Special forces demonstrate counterterrorism skills during a drill conducted by a trilateral air patrol involving Indonesia, Malaysia and the Philippines. THE ASSOCIATED PRESS

Inc., an entity based in the Philippines dedicated to international cooperation.

LOCAL REMEDY

Sometimes threats to the homeland originate in a nation's backyard. For decades, India had been forced to deal with insurgent groups that hide out on Bangladeshi soil. In recent years, however, India's Border Security Force (BSF) and Border Guard Bangladesh (BGB) began sharing intelligence. The pact now has reduced the insurgent threats to "almost zero," K Sharma, director general of the BSF, told *The Indian Express* newspaper.

"Whenever we have information about exodus or insurgents of the northeastern states in Bangladesh, we share the information and immediate raids are undertaken [by the BGB]," he said. "As a result, the number of training places and hideouts of these insurgents have been reduced to almost zero."



A Border Security Force soldier from India looks toward Bangladesh along the banks of the River Brahmaputra. Bangladesh and India have worked together to curb the activities of Indian insurgent groups operating inside Bangladesh.

THE ASSOCIATED PRESS

Bangladesh established permanent camps of border forces in areas where the insurgent groups were operating, the newspaper reported. The insurgents included the National Liberation Front of Tripura, the United National Liberation Front and the United Liberation Front of Assam.

The eradication of their camps was viewed as a major success for the border partnership. Since 2015, the border forces have been conducting coordinated patrols to check for crimes, insurgents and terrorists along the 4,096-kilometer border.

STRONGER TOGETHER

From regional and local partnerships in Southeast Asia to the international sharing of secrets within the Five Eyes alliance, defense and intelligence agreements for decades have thwarted aggression. Some of the most lasting partnerships the world has known were forged by nations fighting together to preserve freedom.

When soldiers from North Korea marched southward on June 25, 1950, they shattered the peace in the Republic of Korea (ROK) with cannon fire and the clatter of automatic weapons. Two days after the fighting broke out, the United Nations asked the world to unite to resist the aggression.

From regional and local partnerships in Southeast Asia to the international sharing of secrets within the Five Eyes alliance, defense and intelligence agreements for decades have thwarted aggression.

Soon, the United Kingdom's 27th Brigade arrived at Pusan to join the ROK and U.S. forces. Shortly after that, troops from Australia, Belgium, Canada, Colombia, Ethiopia, France, Greece, Luxembourg, the Netherlands, New Zealand, the Philippines, Thailand and Turkey arrived. South Africa provided air units, and Denmark, India, Norway and Sweden provided medical units. Italy provided a hospital, even though it was not a U.N. member.

After three years, an armistice was signed to stop the fighting in July 1953, but the U.N. Command remains on the Korean Peninsula. The formation of a binational command between the ROK and the U.S. gives teeth to deterrence efforts. As the ROK's military capabilities improved, it signed an agreement in 1978 with the U.S. to create the ROK/U.S. Combined Forces Command. It has operational control over more than 600,000 active-duty military personnel from both countries. In wartime, augmentation



U.S. Gen. Vincent Brooks, then commander of the United Nations Command, U.S. Forces Korea and the Combined Forces Command, speaks during opening ceremonies for Camp Humphreys in June 2018.

THE ASSOCIATED PRESS

Honor guards from the Republic of Korea (ROK) and the United Nations Command salute a coffin containing the remains of a South Korean Soldier killed during the Korean War. The U.S. and ROK held a mutual repatriation ceremony at Seoul National Cemetery after the remains of Soldiers killed in the conflict were returned by North Korea. THE ASSOCIATED PRESS

could include 3.5 million ROK reservists and additional U.S. forces deployed from outside the ROK.

As the two countries now negotiate with North Korea over its pledge to denuclearize the peninsula, the partners have affirmed their commitment to each other by creating Camp Humphreys, a sprawling complex about 70 kilometers south of the capital. U.S. Forces Korea and the U.N. Command moved there in 2018.

Leaders from both countries stated at the opening of the headquarters that the U.S.-ROK alliance is vital for

safeguarding the peace on the Korean Peninsula and also the stability of the broader Indo-Pacific region.

‘SACRED RESPONSIBILITY’

While the U.S. protects its interests and defends South Korea in the Indo-Pacific, it has enjoyed a 62-year partnership with Canada to defend its own homeland. The North American Aerospace Defense Command (NORAD) celebrated its 60th anniversary in 2018.

The binational command is charged with aerospace warning and aerospace control for North America. When U.S. Air Force Gen. Terrence J. O’Shaughnessy assumed command of NORAD and U.S. Northern Command in May 2018, he spoke about the sacred mission of the defense partnership — protecting each other’s homes.

“There is no doubt that I am joining a combined team that has safeguarded our nations amidst one of the most diverse and challenging security atmospheres in our history,” O’Shaughnessy said. “Thank you for your selfless service and preservation of our sacred responsibility.”

DYNAMIC DEFENSE

NORAD Deputy Director of Operations:

Analytics, all-domain awareness are pillars of homeland strategy

The Watch spoke with Brig. Gen. Pete M. Fesler, deputy director of operations for the North American Aerospace Defense Command (NORAD), to discuss a wide range of homeland defense issues. Gen. Fesler oversees the execution of aerospace warning, aerospace control and maritime warning for North America.

Gen. Fesler has served in a variety of operational, educational and staff assignments, including multiple tours in both the F-15C and F-22A fighter jets as a command pilot. He participated in multiple deployments, including more than 50 combat missions over Iraq. Before his current assignment, he was stationed at Langley Air Force Base, Virginia, where he commanded the most historic wing of the U.S. Air Force, the 1st Fighter Wing.



Brig. Gen. Pete M. Fesler
U.S. AIR FORCE

THE WATCH: What do U.S. military commanders mean when they say homeland defense is “not just an away game” and that “the homeland is not a sanctuary?”

GEN. FESLER: Historically, the U.S. military has fought an away game to prevent conflict from reaching our shores. During the Cold War, our adversaries could reach us in the homeland, but only with nuclear weapons. We deterred a nuclear attack by maintaining a robust and survivable nuclear force. Today our adversaries are circumventing that deterrent capability by fielding systems and training to conduct conventional strikes against the homeland. They’ve told us in open source [publicly available materials] that they intend to horizontally escalate to strikes against the homeland

“After 9/11, we invested heavily in the ability to counter a violent extremist threat. We are well-postured to defend against that threat today.”

in the event of conflicts elsewhere. The adversary is no longer going to allow us to fight an away game. They are taking away our traditional sanctuary here in the homeland.

THE WATCH: The National Defense Strategy says that great-power competition has reemerged as the central challenge to U.S. prosperity and security. Russia has even mentioned potential targets inside the United States. Can you detail some of these new challenges?

GEN. FESLER: Some of the new challenges we face in the homeland include the widely publicized and talked about stealthy Russian submarines capable of launching land attack cruise missiles, modernized long-range bombers and cruise missiles, which themselves are stealthy and have ranges that allow them to be launched from outside of sensor range against targets in the homeland. They’ve even recently discussed the fielding of an intercontinental-range nuclear-armed torpedo. These are things we did not face during the Cold War with the Russians. They are fielding all of these rapidly. Some of them already have been fielded, and some will be fielded in the next couple of years. China is following a similar path, and they are actually moving more quickly than Russia, investing in their own modernized, next generation of submarines. They are investing in bombers and the tanker capacity required to allow those bombers to reach North America, and in the weapons that those bombers will deliver. Even North Korea, as we’ve all seen, is continuing to modernize its intercontinental-range ballistic missile force. Recently, they detonated a thermonuclear device. So now, where we’ve had doubts about the

yield of the weapons they might put on top of the ICBMs [intercontinental ballistic missiles], it’s now clear that they’ve reached the ability to deliver a more than 100-kiloton weapon against any target in North America. These are new challenges that are emerging, and we have to be prepared to defend against them.

THE WATCH: How should the U.S. prioritize its homeland defense investments

to adjust the focus from mainly keying on violent extremist organizations to the threats posed by near-peer competitors, such as the People’s Republic of China and Russia?

GEN. FESLER: After 9/11, we invested heavily in the ability to counter a violent extremist threat. We are well-postured to defend against that threat today. But our adversaries, as I



PETTY OFFICER 2ND CLASS MARKUS CASTANEDA/U.S. NAVY

The amphibious dock landing ship **USS Ashland** launches a **Rolling Airframe Missile (RAM)** during an exercise in the Pacific Ocean. Missile exercises are designed to increase tactical proficiency, lethality and interoperability of participating warships in an era of great-power competition.

An **F-22** fighter jet from the North American Aerospace Defense Command intercepts a Russian **Tu-142** maritime reconnaissance aircraft as it enters the Alaskan Air Defense Identification Zone on March 9, 2020.



NORAD

mentioned, are continuing to develop capabilities and technologies that are designed to challenge our current defenses. Investment in domain awareness, investment in the ability to control a joint force in all domains, and defeat mechanisms are required for us to maintain the advantage that we enjoy now in homeland defense. That investment is occurring right now. Here are a couple of examples: The first one is that we've already initiated the procurement of homeland defense-specific sensors designed to detect cruise missiles, bombers and a wide range of threats. We are rapidly prototyping and fielding a new command-and-control capability that takes advantage of data analytics. Instead of just taking sensor data and pushing that into command-and-control structures, we are now using data analytics to help us understand better what it is that we're seeing. We're modernizing on the service side, too. The Air Force, for example, is modernizing its fighter fleet. That fighter fleet is an important component of our ability to

defend against cruise missiles. They're retiring older platforms like the F-16 and the F-15, and they are replacing them with newer platforms like the F-35 and the F-15EX. And on the ballistic missile defense side, the Missile Defense Agency is developing the next-generation interceptor that will allow us to leapfrog ahead of any technology that a rogue nation is going to be able to field in the future to attack the homeland with an intercontinental-range ballistic missile.

THE WATCH: When military leaders at U.S. Northern Command (USNORTHCOM) and NORAD discuss domain awareness, what does that mean for homeland defense?

“In a recent exercise we used ground-based Army and Marine Corps systems tied in with Air Force airborne sensors to detect, track, identify, and maintain custody of multiple cruise missiles at the same time.”



An F-35A Lightning II flies over Hill Air Force Base, Utah, during training in January 2020. The U.S. Air Force is retiring many of its older platforms, such as the F-15 and F-16, and replacing them with new fighters, such as the F-35 and F-15EX.

GEN. FESLER: The concept of domain awareness is pretty well understood. It simply means understanding what is occurring in any given domain — the air domain, the maritime domain, etc. At NORAD and USNORTHCOM, we use the term all-domain awareness. That means we need to have the ability to understand what's happening in the approaches to North America, from the sea floor to on orbit. Traditionally, we've invested in sensors to counter a single threat. In the 1950s, the Soviet threat was a bomber carrying a gravity-dropped nuclear weapon. So we developed systems to counter that threat, such as the DEW Line [Distant Early Warning Line] — a system of radars stretching from coast to coast and across Alaska and northern Canada. Today, the adversaries are fielding systems that are designed to exploit the seams between each one of our single-threat countering sensors. We have to invest to close those gaps. Investment is required in sensors able to detect, track, and identify and maintain custody of a whole range of threats. We simply can't afford to buy a single sensor to counter a single threat. All-domain awareness is the commander of NORAD and USNORTHCOM's number one priority for investment in homeland defense.

THE WATCH: The U.S. and its partners have talked about the need to integrate air and missile defenses so adversaries do not exploit weaknesses caused by service-centric defense systems. How are we changing our homeland defense investment strategy to meet this challenge?

GEN. FESLER: We are doing this now. In a recent exercise we used ground-based Army and Marine Corps systems tied in with Air Force airborne sensors to detect, track, identify, and maintain custody of multiple cruise missiles at the same time. Those cruise missiles were then handed off to a Patriot missile battalion that successfully engaged and shot them down. In another range of exercises we've conducted over the last six months, we've integrated Navy, Air Force, and space assets to track cruise missiles. Those have all culminated in kills using a variety of new defeat mechanisms. These defeat mechanisms are designed to invert the cost curve and to make the systems that we're firing to shoot down the cruise missiles significantly less costly than the cruise missiles themselves. This is a critical component to being able to defend the homeland against a missed missile attack.

THE WATCH: The U.S. Department of Defense is directing the military services to work together on common frameworks for networks under what it calls Joint All Domain Command and Control. Can you describe this initiative in more detail?

GEN. FESLER: Historically, our command-and-control systems have been service-oriented. A command-and-control structure, for example, might be designed specifically for the Marine Corps or specifically for the Army. And even within those command-and-control systems, we've often designed them for a specific mission set. For example, there is a command-and-control system associated with the Army's air defense systems. But in defending the homeland or more broadly, to successfully



PETTY OFFICER 3RD CLASS MARIANNE GUEMO/U.S. NAVY

conduct modern warfare, we need a command-and-control structure that is able to view all of the forces from all of the services regardless of what theater they're in and bring them to bear. It's more than just the command-and-control systems. Traditionally, we take sensor information, turn it into a picture, make a decision, and then relay command instructions. We're actually moving to using data analytics and artificial intelligence to not only pull in that data but to help decision-makers make a more informed decision using the information that the sensors are providing. That information then gets pushed down to the units that are executing the instructions. By using data analytics and by using a command-and-control structure that spans all of the services, we are now truly able to take information from any sensor and push it to the best shooter.

THE WATCH: U.S. Air Force Gen. Terrence J. O'Shaughnessy, commander of NORAD and USNORTHCOM, has publicly stated that more investment is needed to defend against the threat of cruise missiles. What resources need to be allocated?

GEN. FESLER: What Gen. O'Shaughnessy is talking about is the weight of effort in the defense of the homeland. We've invested heavily in our ability to defeat a violent extremist attack. That investment occurred immediately after 9/11 and has continued in the years since. We spend as much as [U.S.] \$12 billion a year on ballistic missile defense against the North Korean threat, but to defeat cruise missiles we rely on legacy capabilities that are shared between all of the geographic combatant commanders to defend the homeland. That provides a capable defense, but it's inefficient and it's costly. What Gen. O'Shaughnessy has asked us to do is rethink how we're defending the homeland. What we're finding is that upfront investment in purpose-built homeland defense capability ultimately will save resources and still allow us to increase capability. Forces that we free up by using the purpose-built homeland defense capability can then be pushed forward into the away game to bring more forces to bear against an adversary at range.

U.S. Navy Lt. Cmdr. Matthew Eckler tests the Advanced Battle Management System aboard the destroyer USS Thomas Hudner. The system involves cutting-edge technology to detect and eliminate threats from all domains.



THE HIGHEST PRIORITY

A vigorous missile defense strategy is essential to security at home and abroad

THE WATCH STAFF

“We are committed to expanding and improving the state-of-the-art missile defense system to shoot down missiles in flight. We will develop better surveillance and long-strike capabilities to prevent our enemies from launching them in the first place.”

– U.S. President Donald Trump

In congressional testimony in 2019, top United States military officials painted a vivid picture of the evolving threats posed by hostile countries with missile stockpiles. Now more than ever, the military leaders said, the U.S. and its allies must maintain a technological advantage by upgrading the reliability and lethality of missile defense systems.

“The threats facing our nation are not hypothetical,” Gen. Terrence J. O’Shaughnessy, commander of the North American Aerospace Defense Command (NORAD) and U.S. Northern Command (USNORTHCOM), told the Senate Armed Services Committee. “Our competitors’ reach is now global, and they are conspicuously undermining international norms and standards of behavior while possessing the capability to strike targets in North America with both nuclear and advanced non-nuclear weapons launched from well beyond our territory.”

It was just three years ago that the U.S. celebrated a major success by shooting down a mock intercontinental ballistic missile (ICBM) fired from the Marshall Islands in a test of the military’s ground-based midcourse defense

(GMD) system. For the first time, the system destroyed an ICBM-grade target in midair. The success was partly the result of a newly designed guidance system that steered an intercept vehicle into the path of the ICBM, destroying the incoming missile. It was proof that investments in technology can pay big dividends, something O’Shaughnessy emphasized in his testimony.

About 30 countries possess ballistic missiles, of which there are more than 35 variants. While political leaders navigate a diplomatic path to mitigating — or even eliminating — the threat of missile attacks, it remains essential that the U.S. Missile Defense Agency (MDA) continues to expand and perfect its ability to strike airborne threats before they reach our shores or those of our allies and friends.

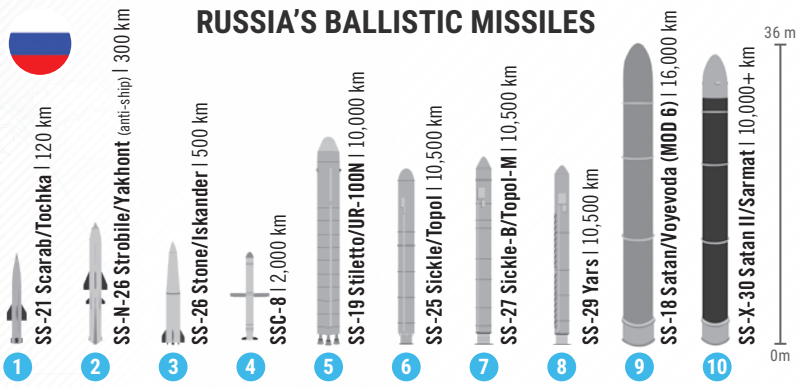
“Diplomacy remains the lead,” O’Shaughnessy said at a gathering of allied air forces. “However, we have a responsibility to our allies and our nation to showcase our unwavering commitment while planning for the worst-case scenario.”

FROM SOVIET BOMBERS TO ICBMS

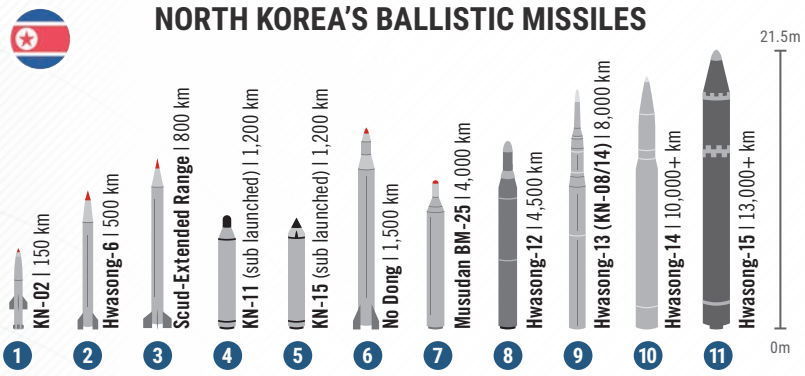
That commitment began in the late 1950s with the creation of NORAD to prevent Soviet bombers from reaching the U.S. and Canada. Forty years later, Congress passed the National Defense Act to protect the U.S. from ICBMs. To support that mission, the MDA has spent U.S. \$132 billion developing the GMD system to identify and intercept airborne threats. It plans to spend another U.S. \$48 billion through 2022.

The goal is to create a system capable of protecting against a wide range of airborne threats — from modern strike aircraft and advanced air- and submarine-launched cruise missiles to small drones. The military will continue to enhance the sensors and guidance thrusters that detect and help destroy incoming missiles. The upgrades fit with the MDA’s mission statement to “develop and deploy a

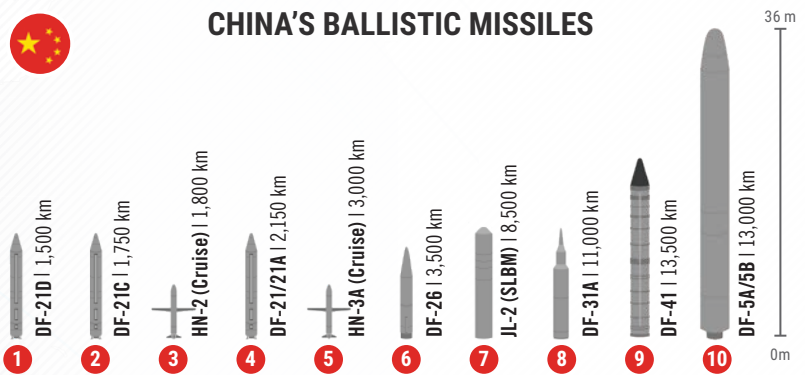




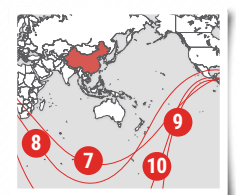
Russia boasts the widest inventory of ballistic and cruise missiles in the world. Moscow's strategic rocket forces perform a variety of missions, including anti-access and area denial of strategic nuclear weapons. Significant modernization efforts include new heavy ICBMs, as well as ground-launched cruise missiles.



North Korea's ballistic missile program is one of the most rapidly developing threats to global security. In recent years, an unprecedented pace of missile testing has included new and longer-range missiles, sea launches and the orbiting of satellites. North Korea has developed two new intercontinental ballistic missiles, the Hwasong-14 and -15, which can likely reach the continental United States.



China has the most active and diverse ballistic missile development program in the world, upgrading its missile forces in number, type and capability. China is modernizing its ICBMs, developing multiple independently targetable reentry vehicles and maneuvering boost-glide vehicles, and has begun deploying a new fleet of nuclear ballistic missile submarines. Short- and medium-range cruise and ballistic missiles form a critical part of its regional anti-access and area denial efforts.





A hypersonic vehicle is released from a booster rocket in this Russian computer simulation. Russia claims that the vehicle, which is launched into space and reenters the atmosphere to cruise at low altitudes, is impervious to U.S. intercept missiles.

THE ASSOCIATED PRESS

A long-range, ground-based interceptor (GBI) is launched from Vandenberg Air Force Base in California. Technological advances are improving GBI systems.

THE ASSOCIATED PRESS



layered ballistic missile defense system to defend the U.S., its deployed forces, allies and friends from ballistic missile attacks of all ranges in all phases of flight.”

Today, the GMD system consists of 44 ground-based interceptors (GBIs) deployed in Alaska and California and connected to land-, sea- and space-based sensors. Technological upgrades are in constant development. “We are strengthening this system and investing in technologies to ensure that we can continue to counter rogue state missile threats to our homeland,” said John Rood, then undersecretary for policy for the U.S. Department of Defense.

A MENACING THREAT MATRIX

It is a given that every advancement in missile defense technology will be countered by advancements in technologies to defeat those defenses. Today, airborne weapons are being designed to fly longer distances with more lethal payloads at altitudes and speeds that challenge detection systems.

“Hypersonic glide vehicles are being developed as a new type of ballistic missile payload,” then-MDA Director and U.S. Air Force Lt. Gen. Samuel A. Greaves told members

of the House Armed Services Committee. “The combination of high speed, maneuverability and relatively low altitude makes them challenging targets for missile defense systems.”

In addition, electromagnetic jamming capabilities and cyber attacks are becoming ever greater threats, while marine launch systems are positioning missiles closer to the U.S. and Canada and to allies across the globe.

At the same time, long-standing threats grow in sophistication.

North Korea’s progress toward developing a nuclear-tipped missile that can reach the U.S. is well-documented, though diplomatic efforts may slow or even reverse its program.

Russia’s missile stockpile is varied and capable of reaching across the U.S. and Canada. It claims to have developed a hypersonic vehicle that can bypass intercept missiles and has already fired next-generation cruise missiles into Syria from ships and submarines. It is also developing stealthy naval platforms to defy detection. “Its new generation of air- and sea-launched cruise missiles feature significantly greater standoff ranges and accuracy than their predecessors, allowing them to strike North America

from well outside NORAD radar coverage,” O’Shaughnessy said. These advancements represent a significant investment by Russia that is likely to put targets at risk in the United States and Canada for years to come.

China claims to have successfully tested a hypersonic aircraft that can reach speeds of 4,500 mph and is investing in mobile ICBMs and ballistic missile submarines. It is increasingly sending ships on intelligence gathering operations outside of its territorial waters, including near the U.S. And Iran has launched ballistic missile strikes in Syria and against U.S. forces in Iraq.

Maintaining a muscular missile defense system is essential to protecting the U.S., Canada, and their allies and friends across the world.

INVESTING IN TECHNOLOGY

To meet the threats, the MDA is improving its missile detection and engagement systems. Adversaries have developed weapons that release debris or decoys that can misdirect the intercept vehicles launched to destroy warheads. The MDA has developed a new radar system — the Long Range Discrimination Radar — that can better sort through the debris. It is one of many technological improvements in development, including lasers to intercept missiles during the boost phase and improved kill vehicles to destroy incoming payloads in space.

Additionally, more GBIs are being put into silos and positioned for firing against incoming threats. Congress appropriated U.S. \$4 billion in 2018 to enhance missile defense capabilities against North Korean threats to the U.S. homeland, forces abroad, allies and partners. The funding means an additional 20 GBIs will be deployed in Alaska as early as 2023.

The ground-based Cobra Dane radar detection system in Alaska and the floating sea-based X-band radar designed to work in heavy seas, both essential to homeland defense, are also being improved.

Even more enhancements can be expected. The Department of Defense’s 2020 missile defense budget request “supports improving the current system and moving toward innovative concepts and advanced technologies,” Rood said. The request also continues the development of defense systems for short-range and midrange missile threats by including additional Patriot missiles and by enhancing the Terminal High Altitude Area Defense (THAAD) system and ship-based Aegis

interceptor systems.

The key is maintaining a flexibility to respond to a crisis wherever it emerges. “We will continue to increase the reliability as well as the capability and capacity of ... missile defense systems and make measured investments in advanced technology to counter the adversary missile threat,” Greaves said.

A VIGOROUS STRATEGY

For the MDA’s part, the focus remains on three main areas, as outlined by Greaves:

- “Increasing system reliability by upgrading, improving and sustaining deployed systems and executing a rigorous and continuous test and evaluation approach with strong modeling and simulation to mature technologies and validated deployed capabilities.”
- “Increasing engagement capability and capacity by increasing the number of fielded interceptors, building out the sensor architecture with the aim of capturing ‘birth-to-death’ tracking, improving system discrimination and integration, leveraging international partnerships for affordability and interoperability, and working closely with the combatant commands to provide integration support and capabilities to meet emergent operational needs.”
- “Addressing the advanced threat by working with combatant commands and Services to address emerging threats, to include the growing and highly challenging hypersonic guide vehicle and cruise missile threats and by pursuing advanced technologies, such as directed energy (which inflicts damage by emitting laser, microwave or particle beams toward a target), and making prudent affordable investments potentially game-changing capabilities.”

CONCLUSION

Maintaining a muscular missile defense system is essential to protecting the U.S., Canada, and their allies and friends across the world. Overcoming the technological advances by adversaries requires a continuous investment in the systems designed to defeat those advances. The Department of Defense budget requests represent a strategy that protects the homeland while protecting overseas forces, allies and partners for years to come.

“Revisionist powers Russia and China have changed global strategic dynamics by fielding advanced long-range weapons systems and engaging in increasingly aggressive efforts to expand their global presence and influence, including in the approaches to the United States and Canada,” O’Shaughnessy testified. “The successful defense of our homeland today relies more than ever on constant vigilance by USNORTHCOM and NORAD, tightly coupled with a reinvigorated emphasis on close integration with our fellow combatant commands, the intelligence community, and our allies and partners.”



COVID-19: U.S. MILITARY MEETS THE CHALLENGE

THE WATCH STAFF

As the COVID-19 pandemic infected hundreds of thousands worldwide in late 2019 and early 2020, the U.S. military aggressively responded by assisting civil health authorities in tasks that ranged from delivering food to building temporary hospitals and deploying medical ships. While agencies such as the U.S. Centers for Disease Control, the U.S. Department of Health and Human Services and the Federal Emergency Management Agency (FEMA) took the lead in the pandemic response, the military support effort involved thousands of personnel and covered all states, territories and Washington, D.C. U.S. Northern Command (USNORTHCOM) leads the 14 Department of Defense COVID-19 operational efforts. "There is nothing more sacred than being right here at home defending the homeland," said Gen. Terrence J. O'Shaughnessy, commander of USNORTHCOM and the North American Aerospace Defense Command. "Our commander in chief has declared war on COVID-19. We are a part of that as a whole-of-America, whole-of-nation approach, and we are incredibly proud to be a part of that mission."

U.S. NATIONAL GUARD DEPLOYED

By early June 2020, more than 46,000 members of the National Guard had been activated across the nation to assist efforts to mitigate and control the COVID-19 pandemic.

The troops supported community-based testing sites, created enhanced medical capacity, provided logistical support and transportation of supplies, and helped state emergency operations centers.

Guard members also helped build medical facilities and worked to clean and disinfect common spaces in hard-hit areas.

All states, under Title 32 status, mobilized their National Guard troops. U.S. Defense Secretary Mark Esper said the Guard units were supporting drive-through testing sites, conducting food delivery to vulnerable populations, and helping states plan and coordinate their local responses.

FLOATING HOSPITALS

FEMA Administrator Peter Gaynor announced in late March 2020 that two U.S. military hospital ships would be deployed to free up local beds for COVID-19 patients. The USNS Mercy traveled from its home port of San Diego, California, to Los Angeles, and the USNS Comfort, which is stationed in Norfolk, Virginia, headed to New York City. The ships, which each have 1,000 beds, originally were not sent to treat coronavirus patients. Mercy "will serve as a referral hospital for non-COVID-19 patients currently admitted to shore-based hospitals and will

Demand for hospital beds to treat coronavirus patients became so great that the Comfort was reconfigured to accept COVID-19 patients as New York became the epicenter of the pandemic in the U.S.

REUTERS

Members of Joint Task Force 2, which is composed of Soldiers and Airmen from the New York Army and Air National Guard, arrive to sanitize and disinfect the Young Israel of New Rochelle synagogue in New Rochelle, New York, as snow falls in late March 2020.

provide a full spectrum of medical care to include critical and urgent care for adults,” Gaynor said, according to a UPI report. “This will allow local health professionals to focus on treating COVID-19 patients and for shore-based hospitals to use their intensive care units and ventilators for those patients.”

Demand for hospital beds to treat coronavirus patients became so great, however, that the Comfort was reconfigured to accept COVID-19 patients as New York became the epicenter of the pandemic in the U.S.

The floating hospitals are staffed by medical and support personnel from the U.S. Navy’s Bureau of Medicine and Surgery. Civil service mariners operate the ships.

FIELD HOSPITALS

The U.S. Army Corps of Engineers announced in March 2020 that it planned to convert more than 10,000 empty hotel and college dorm rooms into hospital rooms to treat COVID-19 cases in New York City and was considering similar operations for Washington and California.

“These hotels are empty. The people don’t have jobs,” Lt. Gen. Todd T. Semonite, chief of engineers and commanding general of the U.S. Army Corps of Engineers, told reporters. “We’ll go in and cut a contract



REUTERS

The USNS Mercy, a Navy hospital ship, departs the Naval Station San Diego and heads to the Port of Los Angeles to aid medical facilities dealing with COVID-19 patients.

and be able to have the state set up a lease for that particular facility, and then we would take the building over. And in an exceptionally short amount of days we would go in and turn this into an ICU-like facility,” he said, referring to hospital intensive care units.

The military response also included the establishment of field hospitals in New Jersey, New York and Washington. The 627th Hospital Center from Fort Carson, Colorado, was deployed to Joint Base Lewis-McChord, Washington, to support medical efforts in the Seattle area. The 531st Hospital Center from Fort Campbell, Kentucky, deployed to Joint Base McGuire-Dix-Lakehurst, New Jersey, to set up a field hospital in New York City, and the 9th Hospital Center from Fort Hood, Texas, deployed to the same base to support New York City.

A 450-person U.S. Navy Medical Unit also deployed to Texas and New Orleans. By early June 2020, the military was supporting 24 hospitals and 11 alternate care facilities across the country. In New York City alone, 797 military medical personnel were embedded in 11 hospitals.

CRITICAL SUPPLIES

As part of the whole-of-government approach to fighting the pandemic, the U.S. Department of Defense (DOD) agreed to provide medical supplies and capabilities to the Department of Health and Human Services. Secretary Esper said in mid-March 2020 that the DOD would release 5 million respirator masks and 2,000 ventilators from its strategic reserves.

Defense personnel planned to train civilian operators on how to use the military’s ventilators because they have distinct differences from those in civilian use.

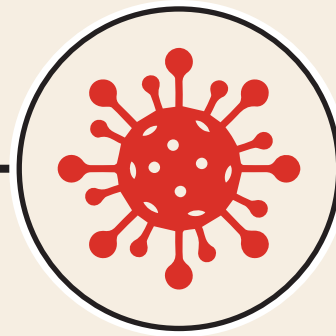
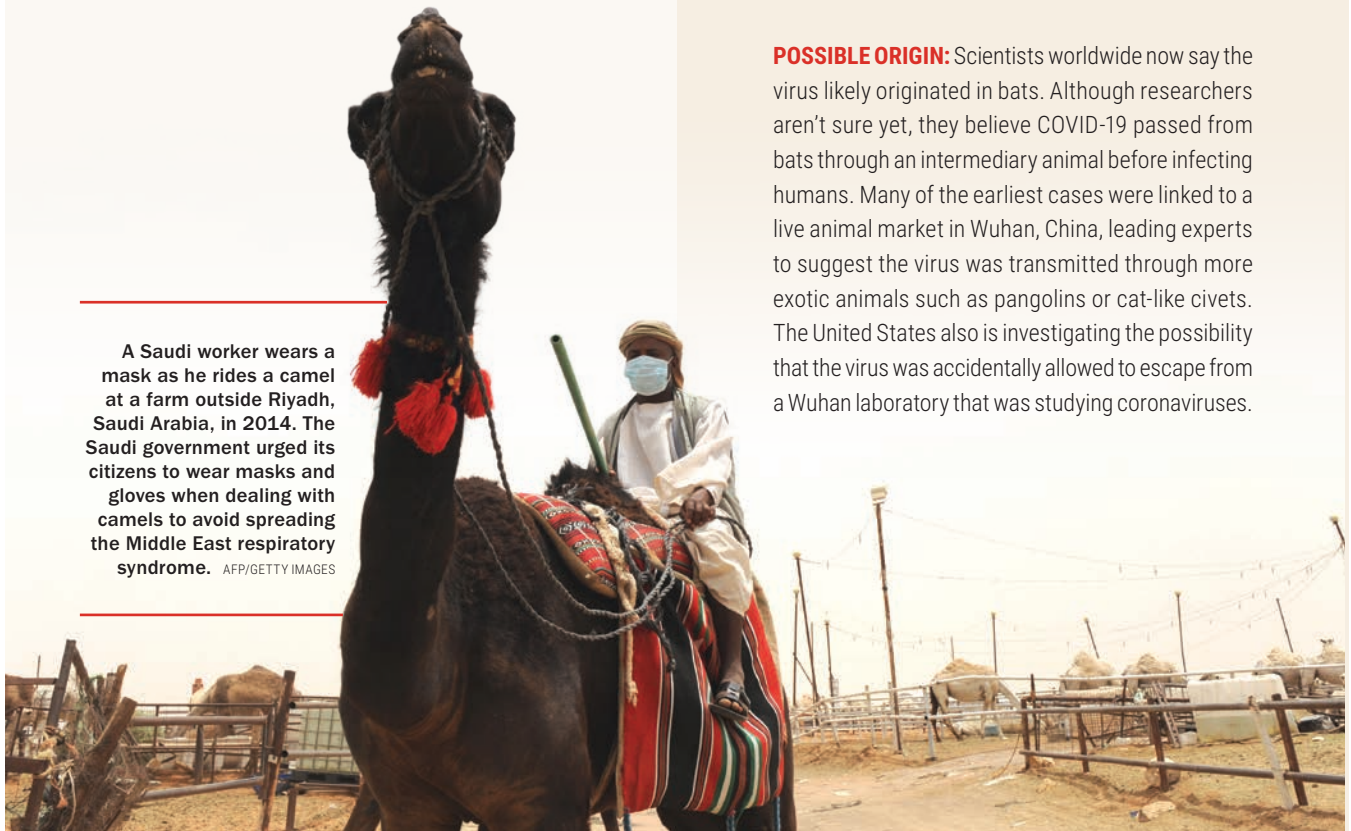
Additionally, the Pentagon said it would make 16 certified testing labs available to nonmilitary personnel to trace the spread of the virus. “I’ve made it clear that we will continue to support the administration’s comprehensive efforts and the country every step of the way, while ensuring our nation’s security remains the top priority of the Department of Defense,” Esper said, according to his department’s website.

CORONAVIRUS OUTBREAKS

THE WATCH STAFF

COVID-19 is from the coronavirus family, which includes viruses that can cause the common cold and serious illnesses such as the severe acute respiratory syndrome (SARS) and the Middle East respiratory syndrome (MERS).

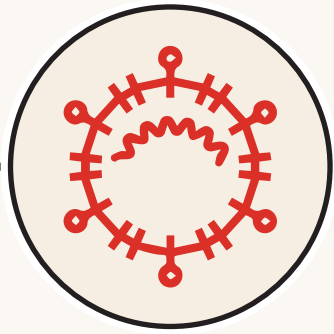
A Saudi worker wears a mask as he rides a camel at a farm outside Riyadh, Saudi Arabia, in 2014. The Saudi government urged its citizens to wear masks and gloves when dealing with camels to avoid spreading the Middle East respiratory syndrome. AFP/GETTY IMAGES



2019

COVID-19 is a new coronavirus that is believed to have originated in Wuhan, China. By early May 2020, COVID-19 had spread to 212 countries and territories, infected more than 4 million people and resulted in more than 270,000 deaths.

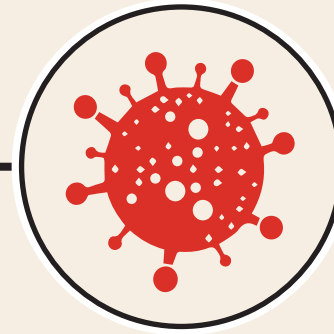
POSSIBLE ORIGIN: Scientists worldwide now say the virus likely originated in bats. Although researchers aren't sure yet, they believe COVID-19 passed from bats through an intermediary animal before infecting humans. Many of the earliest cases were linked to a live animal market in Wuhan, China, leading experts to suggest the virus was transmitted through more exotic animals such as pangolins or cat-like civets. The United States also is investigating the possibility that the virus was accidentally allowed to escape from a Wuhan laboratory that was studying coronaviruses.



2012

MERS was first reported in Saudi Arabia in September 2012 and has since spread to 27 countries. Some people infected with MERS coronavirus develop severe acute respiratory illness, including fever, cough and shortness of breath. Through January 2020, the World Health Organization confirmed 2,519 MERS cases and 866 deaths. About 80% of the cases were diagnosed in Saudi Arabia.

POSSIBLE ORIGIN: MERS is a coronavirus believed to have originated in bats. Humans, however, are typically infected through contact with camels.



2003

SARS was first reported in Asia in 2003 before spreading to a total of 29 countries. The SARS epidemic resulted in 8,096 people becoming infected and led to 774 deaths.

POSSIBLE ORIGIN: Chinese scientists in 2017 traced the SARS coronavirus through the intermediary of civets to cave-dwelling horseshoe bats in Yunnan province, China.

ABOUT COVID-19 THE WATCH STAFF

A global pandemic of respiratory disease spreading from person to person was caused by a novel (new) coronavirus that originated in Wuhan, China. Named coronavirus disease 2019, it is more commonly known by the abbreviation COVID-19.

The virus causes mild to severe respiratory illness. In severe cases, it can be fatal. Although COVID-19 can infect people of all ages, those most at risk of serious illness are 65 and older or have underlying health conditions, such as chronic lung disease, diabetes or serious heart conditions, according to the U.S. Centers for Disease Control and Prevention.

SPACE WASTE

Working together to defend the planet from orbiting debris

THE WATCH STAFF



China tested its anti-satellite capabilities in 2007 by purposely destroying a nonfunctional weather satellite with a surface-launched, medium-range missile. The test created more than 3,300 pieces of debris larger than 10 centimeters in diameter. A collision with any one of these pieces would

prove catastrophic to the average satellite circling Earth or even the International Space Station (ISS), according to the European Space Agency (ESA).

The missile test also produced more than 200,000 debris particles as small as 1 centimeter, large enough to disable a spacecraft or penetrate the ISS shields. Even a collision with a particle smaller than 1 millimeter, such as a fleck of paint, could destroy a satellite subsystem because even those particles travel at more than 24,700 kilometers per hour in orbit.

“Any of these debris have the potential for seriously disrupting or terminating the mission of operational spacecraft in low Earth orbit” about 400 to 2,000 kilometers up, explained Nicholas Johnson, chief scientist at the U.S. National Aeronautics and Space Administration’s (NASA’s) Orbital Debris Program, which was founded in 1979 at Johnson Space Center in Houston, Texas. “This

satellite breakup represents the most prolific and serious fragmentation in the course of 50 years of space operations,” he told space.com after the 2007 test.

Two years later a defunct 950-kilogram Russian satellite known as Cosmos-2251 collided with and destroyed a functioning U.S. Iridium commercial satellite, creating another 2,000 large pieces and more than 100,000 smaller particles. Together, the two incidents increased the amount of debris in low Earth orbit by 60 %, with more than a third of the additional particles remaining in orbit for 20 more years.

In the past decade, the potential threat to satellites from orbital debris has continued to grow. The ESA estimates there are up to 34,000 pieces of space junk bigger than 10 centimeters in diameter; 900,000 objects between 1 to 10 centimeters; and 128 million objects between 1 millimeter and 1 centimeter in size orbiting the planet, for a combined mass of more than 8,800 metric tons — an amount greater than the mass of the metal structure of the Eiffel Tower. The figures include more than 2,500 satellites that are no longer operational but remain in orbit.

To mitigate the threat, the Space Surveillance Network (SSN), now led by U.S. Space Command (USSPACECOM), relies upon a global network of partners to identify, track and share information about space objects. Employing a range of internationally operated satellites, sensors, optical telescopes, radar systems and supercomputers, SSN actively tracks more than 25,000 man-made objects in orbit that are roughly the size of a softball or larger and then warns operators worldwide of pending collisions, according to Diana McKissock, a space lead with the U.S. Air Force’s 18th Space Control Squadron, which tracks space debris for SSN.

In 2017, for example, the U.S. Air Force documented 308,984 potential collisions with active satellites and issued 655 alerts to satellite operators, McKissock told *The Watch*. Operators reposition satellites roughly twice a week based on that information. Chief among the recent space hazards was China’s defunct Tiangong-1 space station that uncontrollably crashed to Earth on April 2, 2018, threatening land-based populations before its fiery demise. Luckily, the debris fell into the Pacific Ocean about 4,000 kilometers south of Hawaii.





International Space Station flight controllers routinely conduct avoidance maneuvers to steer the station clear of space fragments. This image features a night view of the station above Earth's city lights and the green glow of aurora along the outer edge of its atmosphere.

NASA

CROWDED ORBITS

Managing man-made debris created by space missions is increasingly challenging, especially as space becomes more accessible and congested as ambitions grow. Today, 60 governments are operating more than 1,880 active satellites, and 12 countries and one governing body possess launch capabilities, according to the Union for Concerned Scientists, a nonprofit U.S.-based science association. Experts predict the number of satellites in orbit could more than triple over the next decade because an average of 300 satellites with a mass of more than 50 kilograms are now being launched each year, and the pace is expected to accelerate. Within two decades, the number of satellites circling the planet

could increase by a factor of 10 to 16,000 and with it the number of alerts, according to a 2018 policy paper published by the Aerospace Corp.

Space-based systems confer technological, tactical and economic advantages on nations that possess those capabilities in the military and commercial sectors. Satellites enhance navigation, precision targeting, drone operations, communications, and real-time situational awareness on the battlefield and beyond. Some commercial companies such as SpaceX and OneWeb plan to launch thousands of small satellites.

The world's increasing reliance on satellites reinforces the need for fostering cooperation and building partnerships, experts say. "As more space capabilities are launched

continued on page 36

MANAGING THE THREAT

Nations are teaming up to develop ways to remove space debris from orbit, testing many of the systems from the International Space Station (ISS). A consortium of researchers, led by Guglielmo Aglietti, director of the Surrey Space Centre at the University of Surrey, has been developing methods that strive to tether, harpoon or net space junk and bring such debris down to about 200 kilometers above the surface to reenter Earth's atmosphere and be burned up. The RemoveDebris satellite carrying the leading wave of these experiments was deployed from the ISS in June 2018 by the Japanese experiment module's robotic arm to begin a series of tests.

"We have spent many years developing innovative active debris removal systems to be at the forefront of tackling this growing problem of space debris," said Nicolas Charmussy, head of Airbus Space Systems, which developed three of the key technologies aboard the RemoveDebris satellite. "We will continue to work close with teams across the world to make our expertise available to help solve this issue."

Space scientists from various space-faring nations are also working on approaches to create high-powered lasers that can vaporize space junk of all sizes. In 2015, Japanese researchers first proposed focusing small lasers into a beam and mounting them on Japan's module on the ISS or on a satellite to target debris. Researchers at China's Air Force Engineering University in Xi'an, Shaanxi province, proposed using satellite-mounted lasers to blast orbital debris, including pieces less than 10 centimeters wide. They published their approach in a February 2018 article in *Optik*, the international journal for light and electron optics.

Meanwhile, Precision Instrument Systems, which is a research and development branch of the Russian space agency, plans to build a 3-meter optical telescope that can track space junk in orbit and then blast it into oblivion, the Live Science website reported in June 2018.

Mitigating Future Risk

In the future, as space becomes more crowded, space junk could become even more perilous due to the Kessler effect. The notion posited in 1978 holds that as the density of objects in space increases, so does the probability for

collisions between them. In a Kessler syndrome event in a congested orbit, one collision leads to another and another, creating a disastrous chain reaction of collisions of space junk that could close regions of Earth's orbit to satellite traffic altogether.

Most space scientists think this wouldn't happen, if it happens at all, for several decades, however. "I'm not saying we couldn't get there, and I'm not saying we don't need to be smart and manage the problem," Jesse Gossner, an orbital-mechanics engineer who teaches at the U.S. Air Force's Advanced Space Operations School, told the website Business Insider. "But I don't see it ever becoming, anytime soon, an unmanageable problem."

Gossner, McKissock and many other experts think finding, tracking and alerting parties about potential collisions remains the most effective approach to managing debris. "It's just a matter of watching and, with our active satellites that we do control, avoiding collisions," Gossner said. "It becomes a very important problem not just for that satellite, but then for the debris that it would create." And for now, some space scientists contend, the smallest particles, which are not trackable, may do the most damage.

Space debris of all varieties will undoubtedly be a continuing challenge for the international community as space ambitions and dependence grow. "Space is going to be a vulnerable domain, so we're going to have to think of ways to mitigate that risk and mitigate those threats," Elbridge Colby, then a senior fellow at the Center for a New American Security and later Deputy Assistant Secretary of Defense for Strategy and Force Development, told *The Washington Post* newspaper in January 2016.

USSPACECOM will be up to the challenges. U.S. President Donald J. Trump first revealed his plans to revive the command in June 2018. Shortly thereafter, Gen. John Hyten, now vice chairman of the Joint Chiefs of Staff, pledged the space situational awareness mission within the Department of Defense would continue for reasons of national security. "That will not change ... because we have to have that information in order to defend ourselves against potential threats," he said in his June 22, 2018, testimony to the House Armed Services Committee, when he was still head of USSTRATCOM.

The cost of not doing so could be immense. "Every day, we use and rely on services provided by satellites without ever realizing how vulnerable they are," Dr. Hugh Lewis, head of astronautics research at the University of Southampton, told *Wired UK* in April 2017. "It's not just that satellites can be damaged or destroyed by space debris today or tomorrow, it's that the actions of our generation may affect the dreams and ambitions of future generations to work and live in space."

“The space domain is a global resource that is best protected and managed collectively.”

U.S. Air Force Maj. Gen. Nina M. Armagno



worldwide and the number of people benefiting from the use of those systems grows, it is in all of our interests to work together to ensure the security, safety and sustainability of space,” U.S. Air Force Maj. Gen. Nina M. Armagno, director of plans and policy for U.S. Strategic Command (USSTRATCOM), said in April 2018, while the command was still charged with overseeing SSN. “The space domain is a global resource that is best protected and managed collectively.”

INTERNATIONAL COOPERATION

Nations are already working together to improve monitoring capabilities as well as technologies to control space junk. To ensure safe operation in space, USSTRATCOM signed space situational awareness (SSA) agreements with 89 entities, including 14 countries and two intergovernmental agencies to share data. USSPACECOM began assuming management of the agreements soon after the command was stood up in August 2019. The entities include Australia, Belgium, Canada, Denmark, France, Germany, Israel, Italy, Japan, Norway, South Korea, Spain,

SPACE DEBRIS BY THE NUMBERS



Number of rocket launches since the start of the Space Age in 1957:
About **5,600** (excluding failures)



Number of satellites placed into Earth’s orbit:
About **9,600**



Number of these still in space:
About **5,500**



Number of these still functioning:
More than **2,300**



Number of debris objects tracked by Space Surveillance Network:
About **25,000**



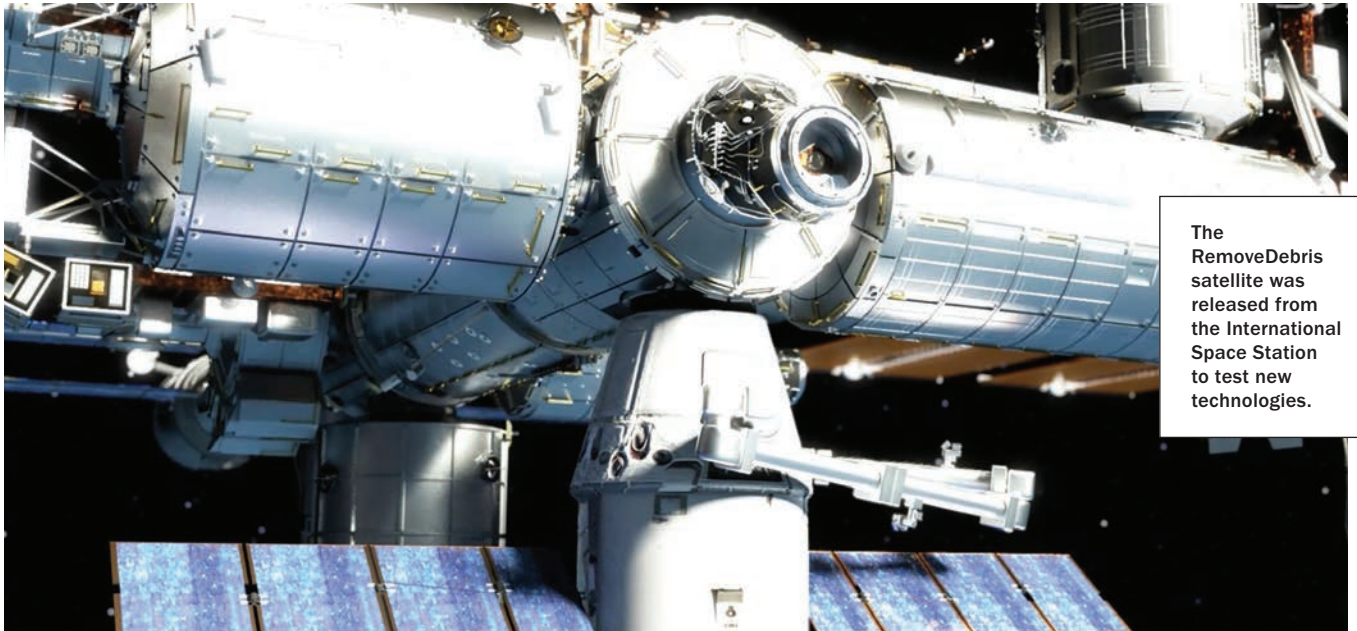
Estimated number of breakups, explosions, collisions or anomalous events each year:
More than **500**



Total mass of all space objects in Earth’s orbit:
More than **8,800** metric tons



Sources: European Space Agency’s (ESA’s) Annual Space Environment Report, February 2020. Figures related to space debris provided by ESA’s Space Debris Office at European Space Operations Centre, Darmstadt, Germany.



The RemoveDebris satellite was released from the International Space Station to test new technologies.

AIRBUS

the United Arab Emirates and the United Kingdom, as well as the European Space Agency and the European Organization for the Exploitation of Meteorological Satellites. USSTRATCOM has been monitoring space junk since 1957 when the Soviets launched Sputnik I. USSPACECOM now also shares information with more than 65 commercial satellite companies and is working to expand the network. “Anyone in the world can request our data,” McKissock told *The Watch*.

The SSA Sharing Program offers collision warning information for the lifetime of a satellite. The Joint Space Operations Center can provide prelaunch information to foreign and commercial operators to prevent collision of space objects with the launch vehicle and payload into early orbit. The program also conducts satellite reentry assessments and can help track asteroid threats, as it did when the 45-meter-wide Asteroid 2012 DA14 passed between Earth and its geostationary satellites in February 2013.

The SSN includes a Space Based Space Surveillance satellite, which orbits at 628 kilometers above the planet, and sensors operated by Australia, Canada, Norway and the United Kingdom, as well as the Space Surveillance Telescope (SST), developed by the U.S. Defense Advanced Research Projects Agency. The SST, which can detect faint objects in geosynchronous orbit up to 35,400 kilometers high, is being moved to Australia from New Mexico to enhance launch detection and tracking in the Southern Hemisphere. In addition, the U.S. upgraded a C-band radar and recently moved it from Antigua Air Station in the Caribbean to Naval Communication Station Harold E. Holt in Exmouth, Western Australia. The radar became operational in 2017.

The SSN also includes the Space Fence System radar, a second-generation space surveillance system designed

to track artificial satellites and space debris in low Earth orbit, which is nearing completion. The initial large S-band radar and facilities were built at Kwajalein Atoll in the Marshall Islands and were declared operational in March 2020. There is an option for another radar site in Western Australia. The enhanced capabilities will enable faster warnings of potential space debris collisions and a greater number — perhaps as many as 200,000 objects, including those down to 4 centimeters in diameter — to be tracked and cataloged.

The international space community also formed the Inter-Agency Space Debris Coordination Committee (IADC) in 1993 to serve as an international governmental forum for the worldwide coordination of activities related to the issues of human-made and natural debris in space. IADC’s members include experts on space debris and other specialists from 13 space agencies, including the Canadian Space Agency, China National Space Administration, European Space Agency, Indian Space Agency, Japan Aerospace Exploration Agency, Korea Aerospace Research Institute and NASA. USSPACECOM also supports IADC’s efforts and those organized by the United Nations Office for Outer Space and its Committee for the Peaceful Uses of Outer Space to address space debris.

Nations are stepping up their contributions to space junk management. Japan added a space monitoring division in 2019 within its Self-Defense Force. “Initially, the force will be tasked with monitoring dangerous debris floating in Earth’s orbit and with protecting satellites from collisions with space debris,” according to *The Japan Times* newspaper. Japan will share information obtained by the new division with the U.S. military to strengthen cooperation in space, the newspaper said.



Ceremonial dynamite charges kicked off the June 1961 ground-breaking ceremony for construction of the Combat Operations Center inside Cheyenne Mountain.

THE STORIED HISTORY OF CHEYENNE MOUNTAIN

Brian D. Laslie, Ph.D.
Photos by NORAD

The idea of a hardened command center is older than the North American Aerospace Defense Command (NORAD) itself. It was January 15, 1956, when Gen. Earle E. Partridge, commander in chief of the Continental Air Defense Command (CONAD), directed his staff to begin preliminary planning for a Combat Operations Center to be located — somewhere — underground. Partridge believed his above-ground center on Ent Air Force Base, Colorado, was too small to manage the growing air defense system and was vulnerable to sabotage or attack by any number of possible, but mainly Soviet, threats.

Partridge and his staff sent preliminary requirements for an underground Combat Operations Center to the headquarters staff of the Air Force in Washington, D.C. The early design, based on a version of the Strategic Air Command headquarters, proposed an above-ground

headquarters, a basement and a three-story underground Combat Operations Center.

Partridge, who was functioning as NORAD commander in April 1958, informed the Joint Chiefs of Staff that his Combat Operations Center should be remote from other prime targets and hardened to continue operating after a thermonuclear blast. He said a Rand Corp. study determined the base location should be in the Colorado Springs area in a granite mountain of the Rocky Mountains.

Partridge said this was the best solution, could be done “at reasonable cost” and should be constructed without delay. The Joint Chiefs of Staff approved locating the new NORAD Combat Operations Center inside Cheyenne Mountain, south of Colorado Springs. The site would include an air and space early warning mission.

It was not until June 1961 that a groundbreaking ceremony was held. Gen. Robert M. Lee of Air Defense Command and Gen. Laurence

On April 20, 1966, Gen. Dean C. Strother, NORAD's commander in chief, transferred NORAD operations from Ent Air Force Base to Cheyenne Mountain and declared the command center fully operational.

S. Kuter, the second commander in chief of NORAD, simultaneously set off symbolic dynamite charges. The estimated cost of the center, including construction and equipment, was set at U.S. \$66 million.

A little more than a year later, excavation of the NORAD Combat Operations Center inside Cheyenne Mountain was mostly completed. It would not be finished, however, until May 1, 1964, principally due to the need to repair a geological fault in the ceiling at one of the intersections by reinforcing it with a massive concrete dome at a cost of about U.S. \$2.7 million. In layman's terms, a giant crack in the ceiling needed buttressing. Thus, a concrete dome was poured and bolted into the ceiling of the hollowed-out mountain. Today the dome can be viewed through a glass partition outside the command center.

Nearly concurrent to these efforts, construction began on interior buildings. Fifteen steel buildings were installed inside the mountain. Each building was separated from the other and mounted on giant springs to absorb shock. Today, the NORAD history office jokingly calls them the real Colorado Springs.

Finally, on April 20, 1966, Gen. Dean C. Strother, NORAD's commander in chief, transferred NORAD operations from Ent Air Force Base to Cheyenne Mountain and declared the command center fully operational.

Once completed, the complex was entered through an access tunnel, itself a preventive measure designed to allow explosive force to flow through the tunnel without damaging internal buildings. To protect the interior command center and buildings, two large sets of blast doors were installed, capable of being closed electronically or by a hand crank, if necessary. Besides the command center, the mountain itself contained everything needed to keep the operations center functioning when sealed off. It had an infirmary, a place to shop and a gym. The operations center functioned as advertised for more than a decade, but events in the latter part of the 1970s nearly led to a catastrophe.

Two events in 1979 and 1980 indicated that exercises and day-to-day missions did not always go according to plan. Unintentionally, these two events helped cement the place of NORAD and the mountain

in American pop culture. First, in November 1979, for about three minutes, a test scenario of a missile attack on North America was inadvertently transmitted to the operational side of the operations center. Test data was processed as real information, displayed on

missile warning consoles in the command post, and transmitted to national command centers. About eight minutes elapsed before NORAD was confident that no strategic attack was underway. Obviously, this aroused widespread public and congressional interest. The second incident occurred eight months later in June 1980. The failure of a computer chip in the NORAD control system caused false missile warning data to be transmitted to Strategic Air Command, the National Command Center and the National Alternate Command Center. These two incidents helped inspire the 1983 film *WarGames*, which itself used the NORAD command center (albeit a highly fictionalized version) as the backdrop for a near-nuclear confrontation.

On the morning of September 11, 2001, the Cheyenne Mountain Operations Center (CMOC) monitored events and directed air defense responses to the terrorist hijackings of commercial airliners and the subsequent crashes. The NORAD commander implemented and conducted Operation Noble Eagle, the air defense response, to the 9/11 events, from the Command Post Battle Cab in Cheyenne Mountain.

In July 2006, the command centers were moved from Cheyenne Mountain to Peterson Air Force Base. Upon completion and review of several studies and reports, Adm. Tim Keating announced the decision to relocate and combine the NORAD Command Center with the command center of U.S. Northern Command (USNORTHCOM) at the headquarters building at Peterson AFB. CMOC officially was renamed the Cheyenne Mountain Directorate and would move to a standby, alternate command center status when further transition efforts over the next year were completed. Today, the Cheyenne Mountain Complex serves as an alternate command center for NORAD and USNORTHCOM.

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



A full moon lights the sky over Cheyenne Mountain outside Colorado Springs, Colorado.

POWERFUL PLANS

Energy generation, resilience are key challenges for military logisticians

THE WATCH STAFF

As the U.S. and its allies prepared to invade Iraq in 2003, nearly 85,000 pieces of cargo and 4,000 containers of ammunition were loaded aboard ships headed for Kuwait from November 2002 to May 2003. The military cargo — enough to fill the deck space of 58 Nimitz-class aircraft carriers — included Abrams battle tanks, Bradley fighting vehicles, Humvees and helicopters. Although the logistical immensity of the six-month buildup was staggering, experts say it pales in comparison to the logistics demands of the future. In future battles, U.S. forces likely would face more technologically sophisticated adversaries, creating environments where military hardware is difficult to protect and communications networks and power supplies can't be taken for granted.

In Operation Iraqi Freedom, the U.S. and its partners did not have to “fight their way to the fight,” wrote retired U.S. Marine Corps Lt. Gen. John E. Wissler in an October 2018 essay for The Heritage Foundation. “Additionally, U.S. and partner-nation forces had significant time to deploy military capability, ultimately using a single point of entry with mature facilities and infrastructure and Internet access.”

In future engagements against sophisticated adversaries, such as the People's Republic of China or Russia, the U.S. and its partners could be forced to battle in environments where communications are degraded and where the supply chain must be decentralized and more maneuverable, Wissler wrote.

PROTECTING THE ENERGY SUPPLY

The U.S. National Defense Strategy requires all services to field ground, air, sea and space forces that can operate, survive and regenerate in all domains while under attack. It's a policy that requires the military to create, distribute and protect energy supplies, defense scholar Mackenzie Eaglen said. Artificial intelligence (AI), big data, robotics and machine learning could revolutionize how future wars are fought, Eaglen said, emphasizing that these technologies all have one critical enabler — electricity. “The military needs a lot more quality energy to power next-generation platforms, sensors, robots, AI and directed-energy weapons for long periods of time,” Eaglen, a resident fellow at the American Enterprise Institute who specializes in defense strategy, defense budgets and military readiness, wrote in a January 2020 article for *The National Interest* magazine.

U.S. Navy officials say they are considering digital “twinning” to create utility and telecommunications replicas for the Pentagon; stationary microreactors for long-term energy resilience; and collaboration with industry to develop small-cell technology and a 5G network for the military.

When evaluating the security of energy resources, three key issues must be addressed, Eaglen told *The Watch*. “First, there is the type of energy generation that is used for installations,” Eaglen said. “This is the most straightforward category, and it encompasses things like generators, reactors, etc. New technology





Fleet replenishment oiler USNS Kanawha, left, sends over a pallet to the guided-missile destroyer USS Carney during a replenishment-at-sea exercise in January 2020.

PETTY OFFICER 1ST CLASS FRED GRAY IV/U.S. NAVY

isn't necessarily needed, just more capacity. Investing in new equipment, like miniature nuclear reactors, could help the U.S. military decrease its dependence on outside utilities."

Energy distribution is another logistical challenge. "It doesn't matter if a nuclear power plant is located near a military base if that base can only connect to the power plant via a USB charger," Eaglen said. "The USB cable cannot deliver enough energy from the plant to power an entire base — even if the energy reservoir is plentiful." This is particularly important for military installations that depend on outside generators and plants, she said.

A third consideration is the need to boost power-generating capacity across military platforms. She pointed to the M1 Abrams tank as an example. New auxiliary power units were installed on the Abrams, "partly because its existing electrical systems failed to fully support the electronics that have been used since the base M1 model," creating a power distribution problem. One of the important challenges the U.S. Navy faces, she said, is that with "railguns

and directed energy laser technology, there's not enough energy available on fleet ships to power these applications. That's an example of a power generation problem."

BUILDING ENERGY RESILIENCE

These logistical challenges have military planners in the U.S. and abroad working diligently to find solutions. U.S. Marine Air Corps Station Miramar, which is just north of San Diego, California, stands out as an example of what energy resilience looks like. The air station received an environmental achievement award in 2019 from the U.S. Department of Defense for establishing power systems that can run for up to three weeks when disconnected from the electrical grid. Miramar constructed a U.S. \$20 million station-wide microgrid that provides 100% renewable energy. The microgrid builds upon energy sources already on the base, including solar power and energy generated from methane gas at landfills. The microgrid supplies backup power and helps the air station reduce utility charges.



U.S. Army Soldiers load an M1A2 Abrams tank onto a fast-transport vessel at the Port of Poti, Georgia.

SGT. 1ST CLASS ROBERT JORDAN/U.S. ARMY

Although Station Miramar stands out for its energy resilience, “it’s not unreasonable to think that many bases can’t operate for even a day or two without an outside power supply,” Eaglen said. “The Pentagon will have to work with outside partners on this massive effort, not compete with them.” That means defense planners in the U.S. and globally need to work with electricity suppliers, telecommunications networks and water providers to build energy resilience in an environment where access to these resources could be limited or cut off.

GETTING TO THE FIGHT

Energy resilience is only one of many challenges facing military logisticians. If a conflict breaks out abroad, the military must transport many tons of equipment and personnel to the battleground. In a crisis, nearly 90% of all U.S. Army and Marine Corps equipment would be carried by ship, according to defense planners. With this requirement in mind, the U.S. military in September 2019 ordered the largest stress test of the Military Sealift Command and

Although the Navy has plans to build new sealift ships, it also has discussed buying more on the open market and retrofitting them to meet the military’s needs.



Maritime Administration in history, activating 33 out of 61 government-owned ships simultaneously. Overall, only about 41% of the ships were fully ready to support a major sealift operation, which demonstrated the need for more investment.

The urgency of investing in the sealift fleet has been on the radar of U.S. military commanders for some time. In March 2019, U.S. Navy Adm. Philip S. Davidson, commander of U.S. Indo-Pacific Command, told the U.S. House Armed Services Committee that Congress must invest more to keep these ships afloat. “Clearly, recapitalization of our sealift system is going to be critically important, as it’s aging out and really has propulsion plants that [are] expiring in capability and our ability to maintain them,” Davidson said. “It’s [a] risk to our troops and all of our people that are forward in the region if there is any delay in our ability to deliver the logistics in accordance with the [operation] plans.”

Although the Navy has plans to build new sealift ships, it also has discussed buying more on the open market and retrofitting them to meet the military’s needs. In addition to the government-owned ships, the Military Sealift Command relies on 125 civilian-crewed surface vessels averaging about 50 years old to replenish Navy ships, conduct specialized missions, and transport personnel, cargo and supplies, according to a news release from the U.S. Department of Defense. “It’s very hard to conduct service-life extensions on a ship that is that old,” said Army Gen. Stephen R. Lyons, commander of U.S. Transportation Command. “What we are finding is the money that



A Humvee is lowered onto the heavy-lift ship MV Ocean Glory in Thailand.

GRADY T. FONTANA/U.S. NAVY



The aircraft carrier USS Harry S. Truman pulls alongside the USNS Supply, a fleet combat support ship, to be replenished with supplies in the Arabian Sea.

PETTY OFFICER 1ST CLASS FRED GRAY IV/U.S. NAVY

is provided against it is woefully insufficient to come back out of the shipyard in a ready status.”

Lyons said he thinks purchasing used ships to augment the fleet is a good solution. “Congress has granted us the authority — granted the Navy the authority — to purchase seven used ships on the open market,” he added. By the end of 2020, the military expects to buy the first two. The Navy’s Military Sealift Command also has prepositioned 15 ships fully loaded with equipment and supplies near likely war zones to reduce response times, according to a January 2020 report in *Forbes* magazine.

WHERE WARS ARE WON

Military history is replete with quotes from generals about the essential nature of sound logistics. Napoleon Bonaparte famously uttered: “The amateurs discuss tactics; the professionals discuss logistics.” In more modern times, Gen. Dwight D. Eisenhower, who would later become the 34th president of the United States, stated, “You will not find it difficult to prove

that battles, campaigns and even wars have been won or lost primarily because of logistics.”

Core logistics functions include the acquisition and distribution of military equipment; the provision of medical services; acquisition of facilities; the provision of food, water and sanitation to the troops; and coordination with overseas partners. Logistics touches every aspect of military might, which is why the U.S. and its partners worldwide are investing the time and money needed to stay one step ahead of their adversaries. “Logistics is the oxygen that allows military muscle to function, grow, and strengthen,” Wissler wrote. “Just as DNA represents the fundamental and distinctive characteristics or qualities of someone or something, logistics planning and modernization define the distinctive characteristics or qualities of the military force and ultimately provide the military commander the freedom of action, endurance and ability to extend operational reach that are necessary to achieve success.”



ARCTIC OCEAN

PARTNERS ASSESS ARCTIC READINESS IN ICEX 2020

THE WATCH STAFF

Five nations and two U.S. Navy fast-attack submarines broke the Arctic ice in March 2020 to assess their operational readiness and train with other services, partners and allies. The Seawolf-class fast-attack submarine USS Connecticut and the Los Angeles-class fast-attack submarine USS Toledo, pictured, conducted multiple Arctic transits, a North Pole surfacing and other training while in the region.

“The Arctic is a potential strategic corridor – between the Indo-Pacific, Europe and the U.S. homeland – for expanded competition,” said U.S. Navy Vice Adm. Daryl Caudle, commander of U.S. Submarine Forces. The forces, he said, “must maintain readiness by exercising in Arctic conditions to ensure they can protect national security interests and maintain favorable balances of power in the Indo-Pacific and Europe if called upon.” Participants from Canada, Japan, Norway and the United Kingdom also contributed to the three-week, biennial exercise.

Ice Camp Seadragon, named for the first U.S. submarine to transit the Northwest Passage in 1960, was established on an Arctic ice floe. It served as a temporary command center for submarine operations and under-ice navigation exercises. The camp also consisted of infrastructure to safely house and support more than 45 personnel. The Navy’s Arctic Submarine Laboratory, based in San Diego, California, served as the lead organization for coordinating, planning and executing the exercise.

JAPAN

JAPAN DEFENSE BUDGET BEEFS UP CYBER, SPACE CAPABILITIES

THE WATCH STAFF

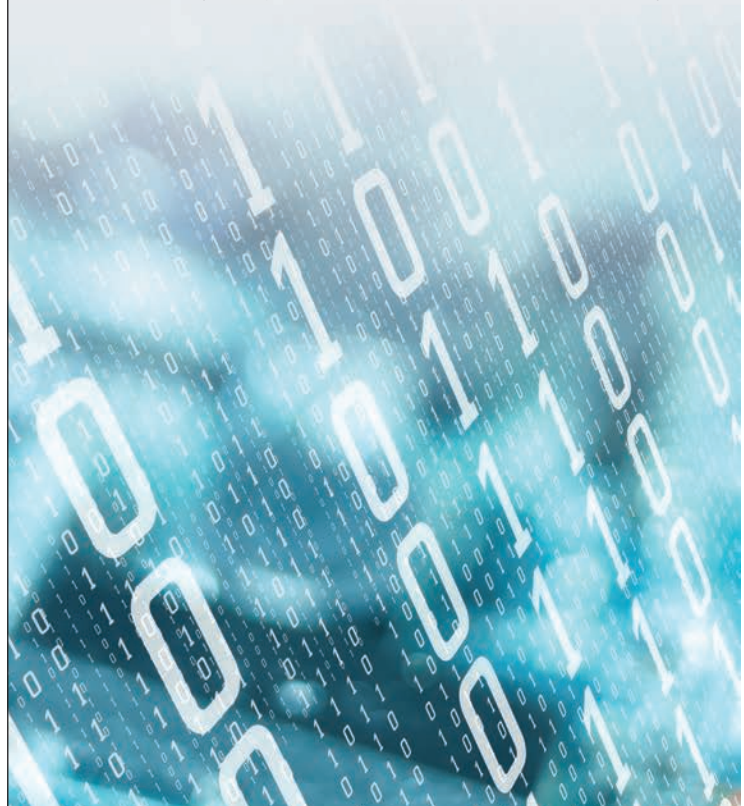
In December 2019, Japan approved a record defense budget of U.S. \$48.5 billion for 2020 with the aim of strengthening the nation’s capabilities in outer space and cyberspace, according to a Kyodo News report.

The draft budget was up 1.1% from fiscal 2019 to a record high for the sixth consecutive year as Japan improves its ability to deal with North Korean missile and nuclear threats and the maritime assertiveness of the People’s Republic of China.

Japan will form the country’s first space operation in 2020 as part of the Air Self-Defense Force. Money will be budgeted for equipment to detect electromagnetic interference with Japanese satellites as well as to monitor space debris.

Japan’s Defense Ministry also plans to expand a cyber defense unit from 220 personnel to 290. Money will be designated to develop a “standoff electronic warfare aircraft,” which can jam the equipment of enemy forces.

Japan’s latest national defense guidelines labeled the cyberspace and outer space defense realms as having the potential to “fundamentally change the existing paradigm of national security.”





UNMANNED AIRCRAFT LIFT NATO CAPABILITIES

Reuters

A cooperative NATO defense project that gives the alliance a state-of-the-art ground surveillance system gained steam in December 2019 with the delivery of the second of five unmanned aircraft to an air base in Italy.

The U.S.-made RQ-4 Global Hawk unmanned aircraft delivered to Sigonella, Italy, is

part of a U.S. \$1.5 billion surveillance system the alliance hopes to have operational in 2022. NATO says the surveillance system will be the world's most advanced and will give the alliance 24-hour, near-real time surveillance of land and sea and provide greater visibility than satellites.

"We are basically creating a small air force," Brig. Gen. Volker Samanns, a senior manager at the NATO program, said. The aircraft can fly for up to 30 hours at high altitude in all weather, seeing through clouds and storms to produce detailed maps, photos and data.

Fifteen NATO allies funded the acquisition of the Northrop Grumman aircraft, including Germany, Italy, Poland and the United States, as well as ground stations built by Airbus. All

29 allies will have access to the intelligence generated, which could include missile sites in Russia, militant activity in the Middle East or pirates off the coast of Africa.

The aircraft will be piloted remotely from Italy and will fly within NATO airspace. It could be flown more widely in a conflict, however. Unmanned or remotely piloted aircraft are increasingly a feature in modern warfare because of their long flying times and intelligence-gathering capabilities.

The delivery of the aircraft underpins Western efforts to remain more technologically advanced than Russia and China, officials said. Brig. Gen. Phillip Stewart, a former Global Hawk commander in the United States, said he did not believe Moscow and Beijing had the sophistication of the NATO system.



DEFENDING CYBERSPACE

NATO countries simulate cyber attacks to boost capabilities

THE WATCH STAFF

In April 2007, Russian hackers incapacitated Estonia's internet with distributed denial of service attacks aimed at government and financial institutions. In August 2008, Georgia, another former subject state of the now-defunct Soviet empire, was hit by similar attacks during an arms invasion by Russian conventional forces. This was the first time cyber attacks were used in coordination with an armed attack as Russia introduced its new "hybrid" warfare model. In March 2014, Russia used similar tactics, but magnitudes greater, when its armed forces seized control of Crimea from Ukraine. And in June 2017, the NotPetya malware attack, which the United States and United Kingdom have attributed to Russia, shut down airports, energy grids, banks and government services in Ukraine.

These are just a few examples of how Russia has used cyber attacks to further its national interests or punish its neighbors for perceived offenses. Other adversarial nations, including the People's Republic of China, North Korea and Iran, have been described as cyber aggressors by U.S. intelligence and security officials. Russia and other adversaries have been working furiously to hack secure government and military networks

of numerous Western countries, including the much-publicized efforts to interfere in American elections, and have been attempting to access Western critical infrastructure networks, such as electrical grids.

In an increasingly digital world, almost every facet of life is connected to networked information systems. More than ever, a robust

In an increasingly digital world, almost every facet of life is connected to networked information systems. More than ever, a robust cyber defense is crucial to defending national critical infrastructure of all types ... in wartime and peacetime.

cyber defense is crucial to defending national critical infrastructure of all types — energy, financial, governmental and military — in wartime and peacetime. Countries such as Estonia and its Baltic neighbors, having already been targeted by Russian cyber attacks, are intimately aware of the threat and are preparing for the worst.

This is why NATO conducts exercises such as Locked Shields 2019, which was held in late April 2019 at the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn, Estonia. It was the largest live-fire cyber exercise hosted by the CCDCOE, incorporating more than 1,200 cyber experts from 30 nations, some in Tallinn and others participating remotely through secure connections from their home countries.

The exercise focused on the fictional country of Berylia, which was experiencing coordinated cyber attacks against a major civilian internet provider and a maritime surveillance system. The attacks disrupted power distribution, 4G communications systems, a water purification system and other critical infrastructure components.

The exercise was designed using the evolving threat landscape and previous years' lessons, addressing areas that have been the most challenging, according to the CCDCOE. It

highlighted the “need for improved dialogue between experts and decision-makers,” the CCDCOE said on its website. “For that purpose, the CCDCOE integrated the technical and strategic game, enabling participating nations to practice the entire chain of command in the event of a severe cyber incident, from strategic to operational level and involving both civilian and military capabilities.”

The French team emerged as the winner of Locked Shields 2019, which the organizers touted as a success. “Locked Shields is a unique opportunity to encourage experimentation, training and cooperation between members of the CCDCOE, NATO and partner nations,” the CCDCOE stated. “It offers an unprecedented opportunity for nations to challenge themselves in an authentic but safe training environment while being aggressively challenged by highly skilled adversaries.”

NATO designated cyber defense as part of its core task of collective defense at the 2014

Russian soldiers without identifying insignia block a road to a Ukrainian military airfield near Sevastopol in Crimea. Russia used massive cyber attacks as part of a hybrid warfare strategy to occupy and annex the Ukrainian territory.

AFP/GETTY IMAGES





Wales summit, meaning that a cyber attack can trigger an Article 5 response by the alliance. Article 5 is NATO's collective defense mandate, which states that an attack on one NATO country is an attack on all. In 2016, NATO put cyberspace on par with land, sea and air domains, making cyber an integral part of NATO operations in all theaters and enabling more focus on training and military planning.

The NATO Computer Incident Response Capability, including its rapid reaction teams, is central to the alliance's efforts to defend its own networks. These resources are also available to help member nations protect their networks. NATO also helps members through information sharing and best practices. The CCDCOE is NATO's go-to resource on research, education and training in the cyber realm.

Locked Shields 2019 demonstrated the



capabilities of the alliance's cyber warriors and helped them improve in their mission to protect critical systems. However, there is no time for complacency. "Cyber attacks can be as damaging as conventional attacks," NATO Secretary-General Jens Stoltenberg said in a speech at the Cyber Defence Pledge Conference in Paris in May 2019. "A single attack can inflict billions of dollars' worth of damage to our economies, bring global companies to a standstill, paralyze our critical infrastructure, undermine our democracies and have crippling impact on military capabilities.

Cyber attacks are becoming more frequent, more complex and more destructive — from low-level attempts to technologically sophisticated attacks. They come from states and nonstate actors, from close to home and from very far away. And, they affect each and every one of us."

A convoy of Russian troops makes its way through the mountains in the direction of Georgia on August 16, 2008. Russia used cyber attacks in coordination with conventional arms when it invaded Georgia.

AFP/GETTY IMAGES

PERFECTING THE KILL CHAIN

THE WATCH STAFF

New technology links sensors, shooters to speed military response



The U.S. military is field testing a new approach to warfighting that breaks down technological and communications barriers to speed up responses to missile attacks. A three-day exercise that demonstrated the Advanced Battle Management System (ABMS) in December 2019 gave military leaders a look at how advanced technology that uses artificial intelligence and machine learning can more seamlessly produce a coordinated response to the cruise missile threat.

“We’re trying to make a system of systems that connects sensors, shooters and C2 nodes with the latest technology, to optimize homeland defense for peer-level conflict,” U.S. Army Maj. Sam Rosenberg, a lead planner on the ABMS team at U.S. Northern Command (USNORTHCOM) and the North American Aerospace Defense Command (NORAD), told *The Watch*.

The ABMS allows warfighters to analyze and share information in real time and orchestrate military operations across all domains — air, land, sea, space and cyberspace. The exercise at Eglin Air Force Base in Florida tested the technology being used to institute the military’s developing concept called Joint All-Domain Command and Control, or JADC2.

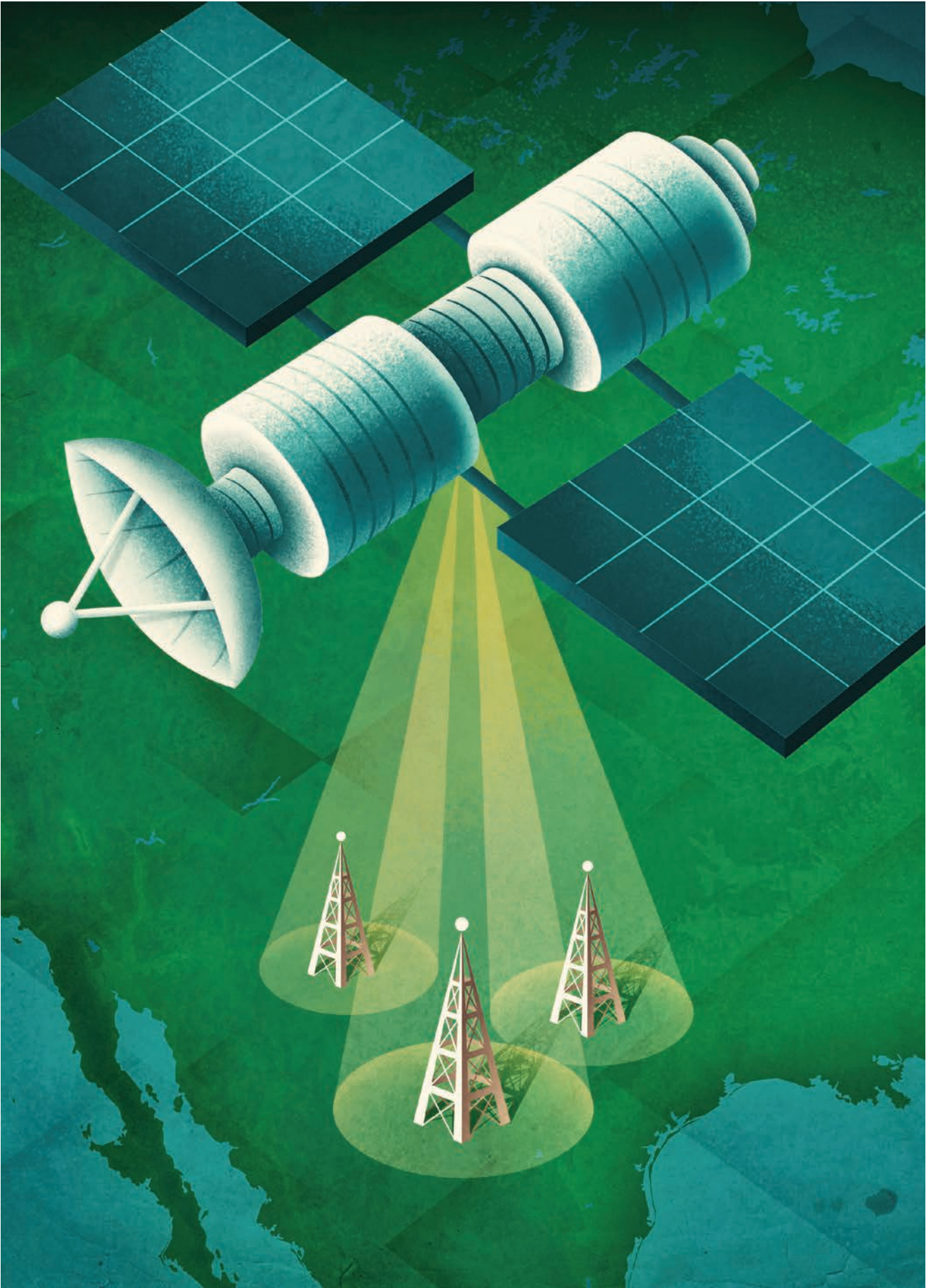
Technology developed by the ABMS team and its industry partners simultaneously receives, fuses,

and acts upon an array of data from all domains in an instant. The initial exercise focused on defending the homeland from a simulated cruise missile attack. “Peer competitors are rapidly advancing their capabilities, seeking to hold our homeland at risk,” said U.S. Air Force Gen. Terrence J. O’Shaughnessy, commander of USNORTHCOM and NORAD, according to a report by the secretary of the U.S. Air Force

“We’re trying to make a system of systems that connects sensors, shooters and C2 nodes with the latest technology, to optimize homeland defense for peer-level conflict.”

– U.S. Army Maj. Sam Rosenberg

Public Affairs. “Working across all of the services and with industry toward solutions to complex problems ensures we meet defense challenges as well as maintain our strategic advantage in an increasingly competitive global environment.”



The ABMS team plans to meet with commanders of geographic combatant commands every four months to address challenges across the globe identified in the National Defense Strategy. The JADC2 concept has been promoted by senior military leaders for three years as a critical warfighting tool, but until recently the idea was confined largely to discussion groups and animated demonstrations, according to the Air Force report. That changed in December 2019 when aircraft from the U.S. Air Force and Navy, a U.S. Army air defense sensor and firing unit, a special operations unit and a Navy destroyer came together to confront and defeat the simulated threat to the homeland.

When the missile threat was detected, new software, communications equipment and a mesh network — networks in which nodes connect dynamically and directly to other nodes — relayed the data to the USS Thomas Hudner, a destroyer deployed in the Gulf of Mexico. The same information was transmitted to a pair of Air Force F-35s and a pair of F-22s. Commanders at Eglin Air Force Base, two Navy F-35s, an Army unit equipped with a mobile missile launcher and special forces on the ground also received the data.

Events culminated on December 18, 2019, when senior leaders from across the Department of Defense (DOD) arrived at the test's command-and-control hub for an ABMS overview and abbreviated exercise. They watched real-time data pour in and out of the command cell. Information flowed instantly and simultaneously across air, land, sea, space and cyberspace. Information came from fighter jets, passing satellites and from sea, and ground forces on the move.

Technological silos of information in which one service's battle systems can't talk to the other has been a key challenge in multidomain operations. The project to develop the ABMS is breaking down those barriers through partnerships with defense industry contractors. In addition to including all military services, the ABMS team is working with 120 agencies and industry partners, Rosenberg said. Private sector partners range from industry giants — Boeing Co. — to tech firms with applicable specialties, such as Immersive Wisdom Inc., a Florida-based company that provides virtual, mixed and augmented reality software, and Anduril Industries Inc., a California-based firm that has assembled a team of experts in artificial intelligence, computer vision, sensor

Members of the 6th Special Operations Squadron use a tablet to upload coordinates during an exercise showcasing the capabilities of the Advanced Battle Management System.

TECH. SGT. JOSHUA GARCIA/U.S. AIR FORCE





1ST LT. SAVANAH BRAY/U.S. AIR FORCE

fusion, optics and data analysis.

Air Force acquisitions lead Dr. Will Roper spoke of the critical need to leverage the expertise of the private sector. “Our four-month ‘connect-a-thon’ cycle unlocks industry’s ability to iterate with testers, acquirers and warfighters,” he said, according to the Air Force report. “For example, the insights from connecting the F-22 and F-35 for the first time will help our industry partners take the next leap.”

Acquisition processes have been greatly expedited for the ABMS project, said U.S. Army Lt. Col. Ian Vargas, a logistics planner. The critical need to share data across platforms and military services “brings the commercial side of the house to the DOD side of the house,” Vargas said, resulting in acquisitions that take weeks or months rather than years.

Military leaders say they want to demonstrate to the troops and the public what the JADC2 concept means for future warfighting. The concept relies on the ABMS team to develop software and algorithms so that artificial intelligence and machine learning can connect

vast amounts of data from sensors and other sources at a speed and accuracy far beyond what is currently attainable.

The ABMS also includes hardware updates for radios and antennas and more robust networks that enable unimpeded data flow to operators. JADC2 also demands a cultural change among service members that responds to multifaceted battlespaces driven by information shared by the joint force.

Achieving this will remove barriers that can keep information from personnel and units. For example, once in place, the new command-and-control ability will allow F-16 and F-35 pilots to see the same information at the same time in the same way a submarine commander sees it. The same information could be viewed simultaneously by a space officer controlling satellites or an Army Special Forces unit on the ground.

“If we get the data piece right, everything will move forward,” U.S. Air Force Gen. John Hyten, vice chairman of the Joint Chiefs of Staff, told audience members at an Air Force

U.S. Air Force Lt. Col. Christopher Laird, an F-35 pilot and commander of the 59th Test and Evaluation Squadron, 53rd Wing, arrives at Eglin Air Force Base for the Air Battle Management System demonstration.



Preston Dunlap, U.S. Air Force chief architect, briefs Department of Defense senior leaders on how the Advanced Battle Management System works during a live demonstration at Eglin Air Force Base in Florida.

TECH. SGT. JOSHUA GARCIA/U.S. AIR FORCE



This leap forward in kill-chain technology is sure to spark dialogue among military partners throughout the world.



Association breakfast in January 2020. “This will be the most important thing we do in the joint force: to figure out how to do that.”

He said the military’s Joint Requirements Oversight Council will move expeditiously to make the JADC2 concept a reality. “I don’t know how that process is going to end up, but I can tell you one thing: It’s not going to be a list of performance criteria that you have to do 10 years from now,” Hyten said, according to a report by the Breaking Defense website. “It’s going to be different. It’s going to focus on how we do things. It’s going to focus on innovation in the services, innovation in industry.”

The process will require the DOD, he said, to allow for flexibility in the development, operation and testing of the new technology — and to allow for failure. “That’s going to be difficult for the department,” he said, “but we’re going to push that, push that really hard.”

This leap forward in kill-chain technology is sure to spark dialogue among military partners throughout the world. What are the engagement criteria? Who gets to shoot? If sensor data is shared across all domains, is there an adequate picture of where friendly forces are deployed to mitigate fratricide? Email your comments to n-nc.peterson.n-ncj3.mbx.the-watch@mail.mil.

ARCTIC ENERGY RESEARCH COULD EXPAND MILITARY REACH THE WATCH STAFF

The U.S. Army and Dartmouth College are teaming up to find ways to better deliver energy to military bases in extremely cold weather.

The partners announced in September 2019 that Dartmouth's Arthur L. Irving Institute for Energy and Society and the Thayer School of Engineering will collaborate with the U.S. Army Corps of Engineers' Cold Regions Research and Engineering Laboratory (CRREL) to look for ways to improve energy delivery, storage and mobility for Arctic military bases.

Energy delivery is central to cold-weather military operations, and the Arctic is drawing international attention for its natural resources and strategic position, according to the CRREL project description.

"CRREL is ramping up in the energy engineering space, and Dartmouth is ramping up in the energy space. So, this is a natural relationship that we really hope to foster and grow over the next couple of decades," said Elizabeth Wilson, the project's principal investigator and director of the Irving Institute, according to Dartmouth's website.

The project aims to extend the Army's mission capabilities by up to 30%.

The partners will undertake three projects. One is to develop a multimodal energy management system that optimizes the supply, demand and storage of energy for an Arctic military base's operation.

A second effort will involve developing high-energy lithium batteries to address the challenges of electrochemical reactions in batteries caused by cold weather.

The third project will be to convert waste heat from power generators into electricity.





REUTERS

U.S. NAVY WANTS LARGER ROBOT WARSHIPS

THE WATCH STAFF

The U.S. Navy wants to work with private industry to build the world's largest unmanned warship.

The Navy wants 10 Large Unmanned Surface Vehicle (LUSV) ships in five years, according to an August 2019 report by *Popular Mechanics* magazine. The ships would serve as scouts for the main battle fleet and would carry sophisticated radar and sonars or floating magazines with extra anti-air and cruise missiles.

The larger unmanned ship would build upon the Navy's experience with Sea Hunter, pictured, an unmanned ship that in 2019 was the first to sail from the mainland to Hawaii. The LUSV will be capable of semi-autonomous or fully autonomous operation.

A report by U.S. Naval Institute News said the Navy asked for U.S. \$400 million in fiscal year 2020 to build two LUSVs that are about 200 to 300 feet long.

If completed, the new LUSV will be the largest unmanned ship to date and will have limited accommodations for a human crew, if necessary.

The ship will be generally unarmed but will have the ability to accept payloads of anti-ship missiles and land attack cruise missiles. In that sense, it will be an extension of the Navy's fleet of destroyers and cruisers.

UNMANNED SYSTEM SETS FLIGHT ENDURANCE RECORD

THE WATCH STAFF

An Israeli company's unmanned aerial system designed for military and homeland defense completed an Israeli record-breaking 25-hour flight in December 2019, according to a report in *The Jerusalem Post* newspaper.

The Orbiter 4 is Aeronautics Ltd.'s most advanced tactical unmanned aircraft system (UAS).

The lightweight system has an operating range of up to 150 kilometers, the company stated. With its endurance capabilities, the UAS extends its intelligence, surveillance, target acquisition and reconnaissance missions.



AERONAUTICS LTD.

The company reported that the Orbiter 4 can be used for artillery fire management and bomb damage assessment, target acquisition for precision-guided weapons, communications intelligence, electronic intelligence and electronic warfare.

Operated by a crew of three, the runway-free aircraft is highly portable and easily deployable. With a low silhouette and silent flight mode, the advanced covert platform is available for both land and maritime operations and can be used in all weather conditions.

ON TARGET WITH MISSILE DEFENSE

Test of next-generation integrated air and missile defense system successful

THE WATCH STAFF



Victory on the battlefield of the future will not necessarily go to the largest or strongest force, but rather to the most agile — to the force that gathers, processes and communicates information rapidly and effectively. The Integrated Air and Missile Defense Battle Command System (IBCS) is a force multiplier that aims to enable the United States and eventually allied forces to do just that.

The IBCS, a “system of systems” in development by Northrop Grumman, is the future command-and-control system for U.S. Army air and missile defense. According to the Army, “a common integrated fire control capability with a distributed ‘plug-and-fight’ network architecture” will be more effective and efficient, allowing air defense units to defend larger areas and reduce the chance of interceptor waste from multiple interceptors engaging the same target.

The IBCS will integrate communications among launchers, sensors and command nodes of all sorts of weapons systems, including missile intercept systems such as the Patriot and the Terminal High Altitude Area Defense (THAAD), the Army’s Indirect Fire Protection Capability, other weapons platforms and combat aircraft. An important multi-domain operations feature of the IBCS is its ability to employ the F-35 fighter as an elevated sensor because it can detect threats that ground-based sensors alone might miss.

The Army conducted a successful intercept test on December 12, 2019, at the White Sands Missile Range in New Mexico where IBCS simultaneously detected, tracked and intercepted two cruise missiles that maneuvered in formation before splitting to attack separate targets. The test used the Sentinel radar, the Marine TPS-59 radar, Patriot air defense batteries and two U.S. Air Force F-35s that contributed to tracking the incoming missiles. The interservice combination of systems demonstrates the essential interoperable IBCS capability of integrating disparate weapons systems.

It was the final developmental flight test before operational testing begins in 2020, according to the Army. IBCS has been in development for some time, but software problems in 2016 and a decision to expand the mission pushed back the deployment date to 2022. Instead of integrating just Army air and missile defense systems, the new mission aims to include multiple sensors across domains to create a layered defense. The system will integrate existing weapons systems as well as new platforms as they are developed.

IBCS is based on the concept of “any sensor, best shooter.” Radars from different systems work together to find and track targets, and “pass the targeting data to whichever launcher is best able to take the shot,” a 2018 article on the Breaking Defense website explained. For example, a Patriot launcher could be in the best place to engage a target not tracked by organic radar, perhaps due to a technical malfunction or enemy electronic warfare, but IBCS would enable



Retired U.S. Air Force Brig. Gen. David Baczewski made a convincing case for a fully integrated NATO air and missile defense capability in an April 2018 opinion column for the Polish website Defence24.com, pointing out that the Russian threat to Poland and other NATO allies in the Baltics is real.

The sun sets over a U.S. Patriot missile defense system in Israel.

AFP/GETTY IMAGES

AFP/GETTY IMAGES



A Terminal High Altitude Area Defense (THAAD) interceptor is launched in July 2017 from the Pacific Spaceport Complex-Alaska. During the test, the THAAD system successfully intercepted an air-launched, medium-range ballistic missile target.

LEAH GARTON/MISSILE DEFENSE AGENCY

the Patriot to take the shot guided by other sensors in the network. IBCS also has the capability to “self-configure as a mobile ad hoc network” as different nodes come on and offline, Northrop Grumman explained during an earlier round of testing in August 2018.

A key feature of IBCS is its use of open architecture design, with “hardware, software and middleware designed as plug-and-play modules that all follow common standards,” according to Breaking Defense. This has allowed IBCS to bypass a common problem in military hardware in which specific software designs for different systems have, for example, made it difficult for different types of Patriots to exchange data.

IBCS will contribute to the agility needed for future threats that the U.S. and allied forces might face. “The recent hostilities between Iran and the United States reinforce the importance of investing in military capabilities,” retired U.S. Air Force Lt. Gen. David Deptula, dean of the Air Force Academy’s Mitchell Institute for Aerospace Power Studies, wrote in a January 2020 article for Breaking Defense. Along with fifth-generation aircraft, such as the F-22, F-35 and B-21, IBCS is an important piece of America’s future defense. “Iran possesses the ability to launch a large volume of missiles against neighbors,” Deptula noted, and IBCS would help counter that ability.

IBCS, initially intended to integrate U.S. Army air and missile defense systems, is now being expanded to include multidomain interoperability across services to include a disparate array of sensors and platforms. It is also being integrated into the Advanced Battle Management System (ABMS) program being led by the U.S. Air Force. ABMS is an ambitious program that also envisions a modular command-and-control system developed with a layered acquisition approach and demonstrated in three yearly

exercises. The next ABMS exercise in September 2020 is designed around a homeland defense scenario and is being operationally led by U.S. Northern Command. The ultimate goal of ABMS is a military internet of things used by all services and allies.

The program could deliver substantial benefits to U.S. partners and allies in forming a collective defense. Retired U.S. Air Force Brig. Gen. David Baczewski made a convincing case for a fully integrated NATO air and missile defense capability in an April 2018 opinion column for the Polish website Defence24.com, pointing out that the Russian threat to Poland and other NATO allies in the Baltics is real. He argued for the NATO-wide adoption of the open system architecture approach incorporated by the IBCS program “to provide an adaptable and readily upgradeable technology basis for both new and legacy systems as well as support the development and integration of future capabilities.”

Poland, perhaps because of its hard-earned familiarity with its large eastern neighbor, has shown a commitment to building a military defense capable of protecting itself and countries nearby. “Poland has become a stalwart member of NATO and a close ally of the United States,” Dan Goure wrote in *The National Interest* magazine. As such, Poland will be the first allied country to acquire the IBCS as part of its air defense system. “A robust, modern, integrated Polish air defense will complicate Russian attack planning and help ensure the survivability of both Polish military units and installations, as well as NATO’s forward-deployed forces,” Goure said. Poland’s acquisition of IBCS should facilitate interest among other allies and partner nations. Its adoption will enhance interoperability among all NATO forces and be a foundation for collective defense in Europe and beyond.



A September 2019 strike by missiles and unmanned aircraft systems damaged the Abqaiq oil processing plant in Saudi Arabia.



AFF/GETTY IMAGES

CONFRONTING AN EVOLVING THREAT

Nations beefing up defenses against unmanned aircraft systems

THE WATCH STAFF

A September 14, 2019, attack on oilfields in Saudi Arabia by 18 unmanned aircraft systems (UAS) and three low-flying missiles temporarily shut down more than 5% of the global oil supply and caused an international spike in fuel prices. More significantly, the attack served notice to homeland defenders worldwide that shoring up defenses against unmanned systems remains a top priority.

The attack, which was attributed to Iran by the United Kingdom and United States, underscored long-held fears of counterterrorism experts about the rapid evolution of inexpensive yet lethal technologies. A September 2019 Bloomberg News report noted that the devices were able to “pierce Saudi defenses in a way that a traditional air force could not: flying long distances to drop potent bombs that apparently set vast portions of the Saudi petroleum infrastructure ablaze.”

Nearly a year before the attack, FBI Director Christopher Wray told a U.S. Senate committee that civilian drones also pose a “steadily escalating threat.” The devices are likely to be used by terrorists, criminal groups or drug cartels, he said, to carry out attacks in the United States.

Homeland defense and security experts are taking notice. From London to Paris to Washington, military researchers, civilian aviation authorities and legislators are confronting the threat. London’s Heathrow Airport announced in January 2020 that it is bringing in a new monitoring system to detect and track drones entering its airspace, *The Daily Telegraph* newspaper reported. Operational Solutions, which makes the technology, said the system will be able to locate the pilot of a drone in any malicious attack.

In Paris, the French company CS Group provided police with its Boreades anti-drone system for use during France’s Bastille Day parade. Also, the operator of Paris’ two main airports, ADP, launched a drone-detection program called Hologarde in partnership with the French aerospace firm Thales.

Military research is also in high gear as defense planners consider options to defend against UAS attacks. One commercially available option is an air launcher that fires a net to capture the drone before dropping it to the ground by parachute. Hijacking UAS signals is another possibility. A U.S.-based company, Department 13, and the Chinese firm Hikvision have developed technologies that can disable an unmanned system or force it to return home. Militaries also are looking at other options, including directional radio frequency interference and laser technology. The U.S. military already possesses Stryker-mounted Hellfire missiles and interceptor drones to knock UAS out of the sky.

Legislative advancements are also part of the arsenal. The U.S. Federal Aviation Administration, for example, issued proposed rules in December 2019 that would require remote identification of UAS by people on the ground or in the air. Within three years of the rule becoming law, nearly all UAS will be expected to communicate their identities and location.

UAS and cruise missiles are difficult to defend against because they fly at low levels, making it difficult for ground-based radar to detect them. They are also mobile, which means the threat can come from missiles launched from the ground, an aircraft, or from ships and submarines.

With many low-cost options commercially available, homeland defenders face a challenge that grows more difficult by the day. “Armed drones and cruise missiles can effectively and efficiently augment a country’s air power and military might, and diversify the threat a potential opponent must defend against,” wrote Peter Brookes, a senior fellow for national security affairs for The Heritage Foundation. “The attack on the Saudis will only make these weapons systems more popular.”



A maintenance craftsman assigned to Travis Air Force Base, California, operates de-icing equipment on a C-5M Super Galaxy during cold-weather training in Alaska.

SENIOR AIRMAN JONATHAN VALDES MONTIJO/U.S. AIR FORCE

CHILLED TO PERFECTION

ALASKAN COMMAND PUBLIC AFFAIRS

Cold-weather training readies maintenance squadrons for difficult missions

A combination of virtual reality training and exposure to bone-chilling Alaskan cold helped Airmen from Travis Air Force Base, California, gain the certifications they needed to perform critical missions in extreme weather conditions.


Joint Base Elmendorf-Richardson (JBER) hosted a five-day training event November 18-22, 2019. Fighter, transport and refueling aircraft were used as part of the de-icing/anti-icing training, which allowed the Airmen to gain the qualifications and certifications needed to de-ice aircraft and vehicles and to perform aircraft maintenance during cold-weather conditions.

A de-icing simulator allowed them to practice their techniques before they were asked to operate the machinery. "It allows an individual who has never operated a de-ice basket to become quite familiar and proficient with the basket controls and overall de-icing operation without feeling the added pressure of maneuvering around an actual aircraft," said U.S. Air Force Master Sgt. Dave Pimentel, 821st

Contingency Response Squadron (CRS) maintenance flight chief assigned to Travis. He also noted how the virtual reality software enables trainees to have an immersive experience and how the simulator can be adjusted to fit any type of weather condition.

Team members who had never performed de-icing operations said the simulator work made the live training less stressful, Pimentel said. The experience becomes priceless when it comes to ensuring maximum readiness for a wide range of potential missions. "The 821st CRS has a multifaceted mission, and this training prepares them for contingencies in an Arctic environment," said U.S. Air Force Master Sgt. Gered Crawford, 732nd Air Mobility Squadron lead production superintendent.

Pimentel emphasized the importance of readiness when it comes to maintaining aircraft in all climates and locations. "The experiences, training and qualifications obtained here at JBER are vital to ensuring our aircraft maintainers are proficient in Arctic environments," Pimentel said.



A C-17 Globemaster III flies over the Chugach Mountains during an aircraft maintenance training exercise in Alaska.

SENIOR AIRMAN JONATHAN VALDES MONTIJO/U.S. AIR FORCE

SHARING KNOWLEDGE

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

CONTRIBUTE TO *THE WATCH*

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

SUBMISSION TIPS

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

RIGHTS

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

FOR A
FREE
SUBSCRIPTION:

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

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

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

THE WATCH

VIEW US ONLINE: THEWATCH-MAGAZINE.COM

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

UNIPATH-MAGAZINE.COM

IPDEFENSEFORUM.COM

ADF-MAGAZINE.COM

PERCONCORDIAM.COM