

FORUM

INTEGRATED DETERRENCE Key to Free and Open Indo-Pacific



features

8 **Commitment, Partnership and Service**

U.S. defense leader shares military's role in nation's Indo-Pacific strategy.

14 **Holistic Approach**

"Integrated deterrence" key to Indo-Pacific peace.

18 **Truths Unknown**

Inability to verify North Korean claims prompts questions about the status of its people, missiles, leadership.

24 **A Dangerous Frontier**

U.S. Space Command adapts to increasingly complex battleground.

28 **Strategic Challenges**

USSTRATCOM commander: Nuclear-capable competitors pose complex threats.

32 **Solving a Swarm of Challenges**

Military, civilian and scientific partners collaborate across Indo-Pacific to counter rising drone threat.

38 **Press Print**

Militaries invest in 3D printing to improve force efficiency and readiness.

42 **Unrestrained China**

Bearing down on India with aggressive lawfare.

48 **Fighting for Digital Freedom**

Competition for dominance over information technology ecosystems underpins the battle between democratic and authoritarian rule.



54 Undersea Cable Wars

Competition for control of submarine networks brings long-term security risks to the surface.

60 Combating Health-Related Cybersecurity Threats

What the virtual world can learn from public health.

departments

4 Indo-Pacific View

5 Contributors

6 Across the Region

News from the Indo-Pacific.

64 Innovations

South Korean researchers create chameleon-like artificial “skin;” Thai researchers develop machine to dispense more vaccines; and a New Zealand entrepreneur takes his space firm public.

66 Contemplations

Researchers create first detailed map of global coral.

67 Parting Shot



ABOUT THE COVER:

Indian and U.S. Soldiers train during the Yudh Abhyas 21 exercise at Joint Base Elmendorf-Richardson, Alaska, in October 2021, as a U.S. Army AH-64D Apache provides air support.

ALEJANDRO PENIA/U.S. AIR FORCE

Dear Readers,

Welcome to Indo-Pacific Defense FORUM's issue on defense frontiers. Throughout the region, allies and partners are investing in their lines of defense to enhance security. New and existing collaborations are underway involving technological innovations, improved coordination, and cooperation to gain strategic advantages in leveraging all elements of national power.

This edition highlights collaborations and explores competition in defense and security and the evolution of technology's role in the battlespace.

The issue begins with a message from United States Secretary of Defense Lloyd Austin on the U.S. commitment to the region and the importance of partnership. He emphasizes we are far stronger, and for far longer, when we work together. Strategic partnerships among like-minded nations are vital in the near- and long-term in dealing with nuclear threats from North Korea, unrest in Myanmar, intimidation from autocratic powers, climate change, and the COVID-19 pandemic.

An article by the FORUM staff advances the conversation on partnership with a spotlight on integrated deterrence. Integrated deterrence is the application of all forms of national power, across all domains, in coordination with the joint force and synchronized with our allies and partners, to deter conflict. We must also implement this mindset in our multinational training and technology sharing to improve communication and foster a better understanding of weapons and systems capabilities.

U.S. Navy Adm. Charles "Chas" A. Richard, commander of U.S. Strategic Command (USSTRATCOM), shares his thoughts on strategic deterrence. The potential for China and Russia to escalate a conflict is fueling an environment of power competition not seen in decades. While the threats evolve, the fundamentals of deterring them remain unchanged. USSTRATCOM's mission to deter strategic attacks and employ forces extends to the Indo-Pacific, further demonstrating our commitment to regional stability and peace.

The proliferation of drones is an emerging threat to that peace as adversaries increasingly use unmanned aerial vehicles to spy on military operations and conduct attacks. Countering drone technologies, as well as exploring the best ways to harness their capabilities, is an increasing part of military modernization planning. A FORUM article investigates the dynamics of this technology that can be either an asset or an adversary.

In every realm, the use of technology comes with benefits and risks. Cyber insecurity and an unregulated internet present their own challenges to enforcing laws and dissuading bad actors. Dr. Sebastian Kevany and Dr. Deon Canyon of the Daniel K. Inouye Asia-Pacific Center for Security Studies discuss these obstacles in combating health-related cybersecurity threats.

We hope these articles encourage regional conversations on pressing issues. We welcome your comments. Please contact us at ipdf@ipdefenseforum.com to share your thoughts.

All the best,
FORUM Staff

IPD FORUM

Defense Frontiers

Volume 47, Issue 2, 2022

USINDOPACOM LEADERSHIP

JOHN C. AQUILINO
Admiral, USN Commander



STEPHEN D. SKLENKA
*Lieutenant General, USMC
Deputy Commander*

JOHN F.G. WADE
*Rear Admiral, USN
Director for Operations*

CONTACT US

IPD FORUM

Indo-Pacific Defense FORUM
Program Manager,
HQ USINDOPACOM Box 64013
Camp H.M. Smith, HI 96861 USA

ipdefenseforum.com

email:
ipdf@ipdefenseforum.com

Indo-Pacific Defense FORUM is a professional military magazine published quarterly by the commander of the U.S. Indo-Pacific Command to provide an international forum for military personnel of the Indo-Pacific area. The opinions expressed in this magazine do not necessarily represent the policies or points of view of this command or any other agency of the U.S. government. All articles are written by FORUM 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 2333-1593 (print)
ISSN 2333-1607 (online)



BRIG. GEN. DEVIN R. PEPPER is deputy director of the Strategy, Plans and Policy Directorate (DJ5), United States Space Command. He is responsible for developing military strategies, issuing strategic guidance, planning military campaigns and contingency operations, and formulating policy in support of combatant commanders' responsibilities outlined in the Unified Command Plan. He enlisted in the U.S. Air Force in 1989 and received his commission through the Officer Training School in 1996. He is a graduate of the U.S. Air Force Weapons School (Space Superiority Squadron) and has commanded at the squadron, group, Air Force wing and Space Force garrison levels. Prior to his current position, he was commander of Buckley Garrison at Buckley Air Force Base, Colorado. **Featured on Page 24**



U.S. NAVY ADM. CHARLES "CHAS" A. RICHARD is the commander of United States Strategic Command and is responsible for the global command and control of U.S. strategic forces. He graduated with honors from the University of Alabama in 1982 before earning master's degrees with honors from Catholic University of America and the Naval War College. He recently served as commander of Submarine Forces in Norfolk, Virginia. Other flag assignments included deputy commander, U.S. Strategic Command; director of undersea warfare at the Pentagon; deputy commander of Joint Functional Component Command for Global Strike at U.S. Strategic Command; and commander of Submarine Group 10 in Kings Bay, Georgia. **Featured on Page 28**



SAROSH BANA is the executive editor of Business India in Mumbai; regional editor, Indo-Pacific region of Germany's Naval Forces journal; and the India correspondent for the Sydney-based cybersecurity journal Asia Pacific Security Magazine. His work focuses on defense and security, cybersecurity, international affairs, policy and strategy, space, power and energy, and environment and conservation. He studied in India, Switzerland and Germany and has been a board member of the East-West Center Association, a Hawaii-based think tank. **Featured on Page 42**



DR. DEON CANYON, a professor at the Daniel K. Inouye Asia-Pacific Center for Security Studies (DKI-APCSS), focuses on crisis management, biosecurity, the Pacific islands region and gray-zone gaming. His cross-disciplinary research concentrates on understanding, managing, controlling and preventing complex and dynamic security threats with innovative approaches. He has authored over 240 publications during his 29 years at several Australian and U.S. universities and institutions, including DKI-APCSS.



DR. SEBASTIAN "BASS" KEVANY, a professor at DKI-APCSS, is a specialist in health security, health diplomacy, health as foreign policy, international relations, epidemics, pandemics and global public health. Within these realms, he is experienced in the fields of monitoring and evaluation, cost-effectiveness analysis, diplomacy, national and international security, conflict resolution, and the use of public health and epidemic control programs to prevent or resolve international conflict. He also has fieldwork experience from more than 100 missions to the Middle East and North Africa, the Pacific islands and Sub-Saharan Africa. **Featured on Page 60**

Join the Discussion

WE WANT TO HEAR FROM YOU!

Indo-Pacific Defense FORUM caters to military and security personnel in the Indo-Pacific region. A product of U.S. Indo-Pacific Command, the quarterly magazine provides high-quality, in-depth content on topics that impact security efforts across the region – from counterterrorism to international cooperation and natural disasters.

Indo-Pacific Defense FORUM offers extensive content online, with new articles posted daily at www.ipdefenseforum.com

Visitors can:

- Access exclusive online content
- Browse back issues
- Send us feedback
- Request a free subscription
- Learn how to submit articles

INDO-PACIFIC DEFENSE
FORUM

DOWNLOAD OUR APP!



Search "FORUMNEWS" on iTunes or Google Play stores to download the free app.



Join us on Facebook, Twitter, Instagram and WhatsApp: @IPDEFENSEFORUM
See back cover.

Defense Transfer Deal Signed, Elevating Partnership

Japan can now give defense equipment and technology to Vietnam under an agreement signed in September 2021, as the two countries step up their military cooperation amid worries about China's growing military influence.

Japanese Defense Minister Nobuo Kishi, pictured, said the deal elevates their defense partnership "to a new level" and that Japan and Vietnam plan to deepen defense ties through multinational joint exercises and other means.

Japan's Defense Ministry said in a statement that Kishi and his Vietnamese counterpart, Phan Van Giang, agreed on the importance of maintaining freedom of navigation and overflight in the Indo-Pacific region, as well as cooperation in various defense areas including cybersecurity.

Tokyo regularly protests the Chinese coast guard's presence near the Japanese-controlled Senkaku Islands, which the People's Republic of China (PRC) also claims and calls Diaoyu. Japanese officials say Chinese vessels routinely violate Japanese territorial waters around the islands, sometimes threatening fishing boats.

During the talks with Giang, Kishi expressed Japan's strong opposition to "any unilateral attempts to change the status quo by coercion or any activities that escalate tensions," referring to the PRC's increasingly assertive activity in the East and South China seas but without identifying any country by name.

Vietnam is the 11th nation with which Japan has signed a defense equipment and technology transfer deal. Tokyo is looking to expand military cooperation beyond its longtime ally the U.S. and has signed similar agreements with Australia, Indonesia, the Philippines and the United Kingdom. *The Associated Press*

JAPAN, VIETNAM



BLAZING NEW PATH WITH SUBMARINE TECHNOLOGY

SOUTH KOREA

South Korea's development of a conventional submarine-launched ballistic missile (SLBM) is a groundbreaking move, analysts said, with implications for North Korea, South Korea's alliance with the United States and even the prospect of nuclear weapons in South Korea.

South Korea's first underwater-launched ballistic missile is test-fired from a 3,000-ton submarine in South Korean waters September 15, 2021.

THE ASSOCIATED PRESS

In September 2021, South Korea conducted ejection tests of the SLBM from its recently launched Dosan Ahn Chang-ho KSS-III submarine, showcasing a unique capability, South Korean news agency Yonhap reported. It is the only nation to field such weapons without nuclear warheads.

Seoul said the conventionally armed missile is designed to help counter any attack by North Korea. Analysts said the weapon also checks many other boxes for South Korea, including providing a foundation if it decides to pursue a nuclear arsenal.

South Korea's sub-launched missile, believed to be a variant of the country's ground-based Hyunmoo-2B ballistic missile, with a flight range of about 500 kilometers, is smaller than the nuclear-tipped SLBMs developed by the North.

H.I. Sutton, a specialist in military submarines, said the South's technology is more advanced, however, and called the combination of an SLBM with the submarine's quiet air-independent propulsion system a potential "game changer." "In these respects, it is the most potent conventionally powered and armed submarine in the world," he wrote in a report for Naval News.

The SLBM is one of a range of conventional missiles that South Korea is developing to augment its Overwhelming Response doctrine, said Ankit Panda, a senior fellow at the U.S.-based Carnegie Endowment for International Peace. The doctrine is an operational plan for strikes to preempt a North Korean attack or incapacitate its leadership in a major conflict.

The U.S. removed its battlefield nuclear weapons from South Korea in 1991 but continues to protect its ally under a "nuclear umbrella." *Reuters*



Anti-Smuggling Agency *Seizes U.S. \$2.7 Billion* in Afghan Heroin

Indian officials said they seized nearly 3 tons of heroin originating from Afghanistan and worth an estimated U.S. \$2.72 billion in mid-September 2021, amid the chaos following the Taliban's August 2021 takeover of the country.

Afghanistan is the world's biggest illicit opiate supplier, but the Taliban have said they plan to ban the drug trade, without giving details.

Officials arrested two people in connection with the haul and said investigations were ongoing.

India's top anti-smuggling agency, the Directorate of Revenue Intelligence, seized two containers at western Gujarat's Mundra Port after receiving intelligence they contained narcotics, an official said. The containers had been imported by a firm in the southern

coastal city of Vijayawada.

The "investigation conducted so far has also revealed the involvement of Afghan nationals, who are under investigation," the official said.

The narcotics were headed to Delhi, and the two arrested people had sought an import-export license based on a house address in Vijayawada, police said in a statement. Reuters

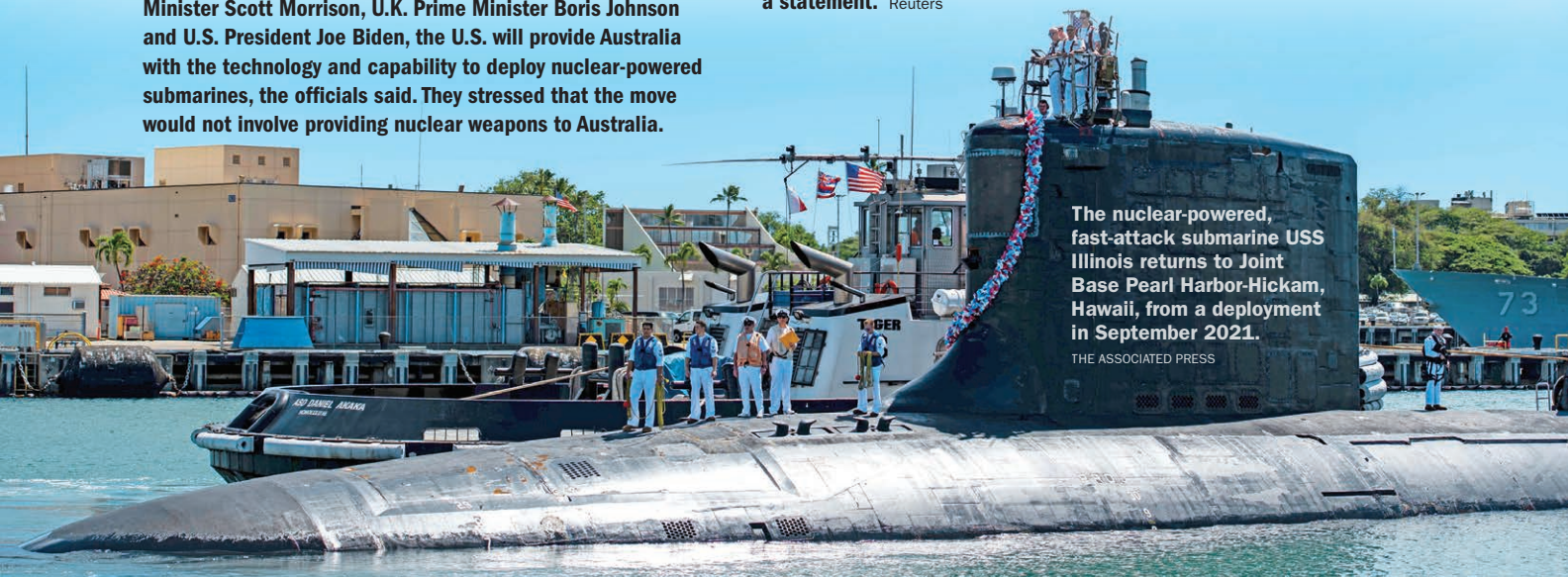
SECURITY PARTNERSHIP TO SHARE NUCLEAR SUBMARINE TECHNOLOGY

Australia, the United Kingdom and the United States established a security partnership, known as AUKUS, for the Indo-Pacific that will involve helping Australia acquire nuclear-powered submarines, senior U.S. officials said in mid-September 2021, as the People's Republic of China's influence in the region grows.

Under the partnership, announced by Australian Prime Minister Scott Morrison, U.K. Prime Minister Boris Johnson and U.S. President Joe Biden, the U.S. will provide Australia with the technology and capability to deploy nuclear-powered submarines, the officials said. They stressed that the move would not involve providing nuclear weapons to Australia.

The officials said the submarines would not be deployed with atomic weaponry but would allow the Royal Australian Navy to operate more quietly, for longer periods, and provide deterrence across the Indo-Pacific. They said the partnership, which will also involve cooperation in areas including artificial intelligence, quantum technology and cyber, was "not aimed at any one country."

"This partnership will become increasingly vital for defending our interests in the Indo-Pacific region and, by extension, protecting our people back at home," Johnson said in a statement. Reuters



The nuclear-powered, fast-attack submarine USS Illinois returns to Joint Base Pearl Harbor-Hickam, Hawaii, from a deployment in September 2021.

THE ASSOCIATED PRESS



COMMITMENT, PARTNERSHIP AND SERVICE

U.S. Defense Leader Shares Military's Role In Nation's Indo-Pacific Strategy

• LLOYD AUSTIN/U.S. DEFENSE DEPARTMENT •

U.S. Secretary of Defense Lloyd Austin delivered this speech while visiting Singapore in late July 2021 on a Southeast Asia trip that included stops in the Philippines and Vietnam. It marked the first articulation of the U.S. Defense Department's role in the nation's Indo-Pacific strategy under U.S. President Joe Biden.

It's great to be here in Singapore, and it's an honor to be giving what I'm told is the 40th Fullerton Lecture. IISS [International Institute for Strategic Studies] has done an outstanding job enriching our dialogue about the Indo-Pacific. Now, we are meeting in difficult times, but we're working with our friends so that we all come out of the pandemic stronger than before.

I'm here to represent a new American administration but also to reaffirm enduring American commitments. Above all, I want to talk about the strategic imperative of partnership.

You know, I learned a core lesson over four decades as a Soldier, in peace and in war: Nobody can go it alone, at least not for very long. We are far stronger, and for far longer, when we come together than when we let ourselves be split apart. The United States and this region are more secure and more prosperous when we work together with our allies and partners.

Together with our friends, we face a range of challenges in this region that demand common action. There are transnational threats, like the pandemic and

the existential threat of climate change, the specter of coercion from rising powers, the nuclear dangers from North Korea, the struggles against repression inside countries such as Myanmar, and leaders who ignore the rule of law and abuse the basic rights and dignity that all people deserve. We will meet those challenges together.

I've come to Southeast Asia to deepen America's bonds with the allies and partners on whom our common security depends. Our network of alliances and friendships is an unparalleled strategic asset. I never take an ally for granted. Together, this region can rebuild from the pandemic and move forward to an even brighter future, in an even stronger rules-based international order. That means more security, more stability, more prosperity, more resilience and more openness.

We're proud to renew a long-standing, bipartisan belief that our partnerships are especially vital in times of great challenge and change. All our countries have suffered from COVID-19, and it is still taking a terrible toll.

Yet, the Indo-Pacific has been tested before. Our recent history has been marked by grave crises — and



U.S. Defense Secretary Lloyd Austin, front, and Singaporean Minister of Defence Dr. Ng Eng Hen pass an honor guard during Austin's July 2021 visit to Singapore to reaffirm the U.S. military's commitment to the Indo-Pacific region.

CHAD J. MCNEELEY/U.S. DEPARTMENT OF DEFENSE

Republic of Singapore Navy stealth frigate RSS Intrepid, foreground, and U.S. Navy guided-missile cruiser USS Shiloh steam together while operating in the South China Sea in June 2021.

SEAMAN OSWALD FELIX JR./U.S. NAVY



by inspiring efforts to tackle them in common purpose. We've seen it over and over again, from the aftermath of World War II, to the frost of the Cold War, to the panic of the 1997 financial crisis, to the ravages of the 2004 tsunami. Yet, at so many key junctures, the countries of the Indo-Pacific resisted the temptation to turn inward and instead forged strong ties and built a more inclusive and secure and prosperous region.


Today, amid this merciless pandemic, we stand together at another hinge moment, and we face another choice between the power of partnership and the dangers of division. I am confident that — through our collective efforts — the Indo-Pacific will again rise to the challenge. And America will be right at your side, just as an old friend should.

Airman Trung Nguyen, from Ho Chi Minh City, Vietnam, assigned to the Golden Falcons of Helicopter Sea Combat Squadron 12, signals an MH-60S Seahawk to land on the flight deck of the U.S. Navy aircraft carrier USS Ronald Reagan in May 2021.

PETTY OFFICER 2ND CLASS
SAMANTHA JETZER/U.S. NAVY



Vietnamese Defence Ministry staff welcome Austin, left, to Hanoi in July 2021. CHAD J. MCNEELEY/U.S. DEPARTMENT OF DEFENSE



After COVID-19, we don't believe that the goal should just be to return to the way that things were. We stand ready to work together, as U.S. President Joe Biden says, to "build back better." The central question for us all is: How can we unite to recover and to rebuild? And how do we work hand in hand to forge a more resilient regional order? We think that the answer involves three components — and all of them are rooted in the imperative of partnership.

- **First**, the most urgent task is recovery. We must redouble our fight against COVID and raise up a safer, healthier and more prosperous future.
- **Second**, we must look further ahead and invest in the cooperation and the capabilities and the vision of deterrence that will meet the security challenges here in Southeast Asia and across the Indo-Pacific.
- **Third**, we must recommit ourselves to the great, long-term project of coming together as Pacific states to build a free and open region, one that stretches toward new horizons of partnership, prosperity and progress.

Let me talk a bit more about those three areas. First, recovery. We must focus on the fundamentals: working urgently together to tackle the COVID crisis and to restore the region's economic dynamism. The pandemic has reminded us how deeply our world is interwoven. Today, a threat to global health anywhere is a threat to security everywhere.

The U.S. has been rushing urgently needed assistance across the Indo-Pacific. That includes testing equipment, oxygen supplies, PPE [personal protective equipment], ventilators and storage for vaccines. My team has been pushing hard to find other ways to help, including providing logistics support, establishing mobile clinics and offering new military medicine training.

But global recovery requires global vaccination. We are rushing lifesaving vaccine doses to the region. President Biden has committed to deliver more than 500 million (later increased to 1.1 billion) shots worldwide over the next year, and the Indo-Pacific is a top priority. We'll keep working to end this plague, for everyone and everywhere. We've watched with admiration as countries across this region have come together to fight it.

When India was besieged, its friends stepped up. We salute Singapore for rushing to the scene, with two C-130s cargo planes carrying some 250 oxygen cylinders. And Singapore has three new vaccine-production facilities planned or under construction, which will help more rapidly deploy vaccines throughout the region in future crises.

Meanwhile, through the Quad's vaccine initiative, Australia, India, Japan and the United States have committed to producing and delivering a billion vaccine doses, right here in the Indo-Pacific. And South Korea is aiming to produce up to a billion vaccine doses this year. To help, South Korea and the U.S. have established a comprehensive Global Vaccine Partnership.

The pandemic is still raging. The road to recovery will be long. These partnerships reflect our common determination and our common humanity. That brings me to the second way that our teamwork can create an even stronger region, and that is by coming together to tackle current and emerging challenges in the region that is the highest strategic priority for the Department of Defense.

Now, President Biden has made clear that the U.S. will lead with diplomacy, and the Department of Defense will be here to provide the resolve and reassurance that America's diplomats can use to help prevent conflict from breaking out in the first place. As I've said before, it's always better to stamp out an ember than to try to put out a blaze.

Deterrence remains the cornerstone of American security. For decades, we have maintained the capabilities, the presence and the relationships needed to ward off conflict and to preserve the stability that lies at the heart of our shared prosperity. Emerging threats and cutting-edge technologies are changing the face and the pace of warfare. We are operating under a new, 21st century vision that I call "integrated deterrence."

Integrated deterrence means using every military and nonmilitary tool in our toolbox, in lockstep with our allies and partners. Integrated deterrence is about using existing capabilities and building new ones and deploying them all in new and networked ways, all tailored to a region's security landscape, and in growing partnership with our friends. Together, we're aiming to coordinate better, to network tighter and to innovate faster. We're working to ensure that our allies and partners have the capabilities, the capacities and the information that they need.

With our friends, we are stepping up our deterrence, resilience and teamwork, including in the cyber and space domains.

We're working with our hosts here in Singapore to enter a new phase in cyber-defense cooperation. We're partnering with Japan to deploy new sensors in space to better detect potentially threatening behaviors — and exploring similar opportunities with other friends.

I'm especially pleased that Singapore has chosen to invest in the F-35 Joint Strike Fighter. That's going to boost our collective capabilities and open up new opportunities for high-end combined training.



Austin, left, meets with Philippine President Rodrigo Duterte in Manila in July 2021 to discuss bilateral relations.

CHAD J. MCNEELEY/U.S. DEPARTMENT OF DEFENSE



gray zone, where the rights and livelihoods of the people of Southeast Asia are coming under stress. That's why we're working to strengthen local capacity and to bolster maritime-domain awareness, so that nations can better protect their sovereignty as well as the fishing rights and the energy resources afforded them by international law.

Meanwhile, we're improving interoperability across our security network. That includes more complex exercises and training. In Japan, for example, we recently wrapped up an ambitious, large-scale exercise, in which U.S. and Japanese forces together conducted the first successful firing of a High Mobility Artillery Rocket System in Japan.

We recently held the exercises known as Pacific Vanguard and Talisman Sabre off the coast of Australia, together with Australia, Japan and the Republic of Korea. That underscored our ability to carry out integrated, high-end maritime operations with our allies.

I'm especially encouraged to see our friends building stronger security ties with one another, further reinforcing the array of partnerships that keeps aggression at bay. Meanwhile, we are working with Taiwan to enhance its own capabilities and to increase its readiness to deter threats and coercion, upholding our commitments under the Taiwan Relations Act and consistent with our one-China policy.

At the same time, we're moving to enhance our


Integrated deterrence also means working with partners to deter coercion and aggression across the spectrum of conflict, including in the so-called

combined presence in the Indo-Pacific with other close partners and allies. Take Britain's historic deployment of a carrier to the Pacific. The HMS Queen Elizabeth is sailing through this region as the flagship of a multinational carrier strike group that includes a U.S. destroyer and a U.S. Marine Corps F-35 squadron.

All that brings me to the final way in which we can move forward together toward the future that this region deserves. I speak as a representative of an Indo-Pacific country with vital interests that are best served by a stable, open and prosperous region. Our strategic partnerships can carry us all closer to the historic common project of a Free and Open Indo-Pacific, at peace with itself and with the world — a stronger, more stable regional order where countries resolve disputes amicably and uphold all the rights of all their citizens.

To bring that day closer, we are working through old alliances and through new partnerships and through regional and multilateral channels — from ASEAN [Association of Southeast Asian Nations] to the Quad to the United Nations Security Council.

We have long sought to create space for Indo-Pacific countries to realize their highest aspirations and safeguard the rights of their citizens. These joint efforts with our friends rely on more than just intersecting interests. They draw strength from common principles — that means a deep belief that countries must remain sovereign and free to chart their own destinies; a profound commitment to transparency, inclusion and the rule of law; a dedication to freedom of the seas; a devotion to human rights and human dignity and human decency; an adherence to core international commitments; and an insistence that disputes will be solved peacefully. Yet, this region has witnessed actions



Instructors drill students from the Bahamas, Malaysia, the Philippines and Thailand at the U.S. Special Operations Command's Naval Small Craft Instruction and Technical Training School in Mississippi in August 2021.

MICHAEL WILLIAMS/U.S. NAVY

that just don't line up with those shared principles.

Beijing's claim to the vast majority of the South China Sea has no basis in international law. That assertion treads on the sovereignty of states in the region. We continue to support the region's coastal states in upholding their rights under international law. We remain committed to the treaty obligations that we have to Japan in the Senkaku Islands and to the Philippines in the South China Sea.

Unfortunately, Beijing's unwillingness to resolve disputes peacefully and to respect the rule of

law isn't just occurring on the water. We have also seen aggression against India, destabilizing military activity and other forms of coercion against the people of Taiwan and genocide and crimes against humanity against Uyghur Muslims in Xinjiang. Now, these differences and disputes are real, but the way that you manage them counts. We will not flinch when our interests are threatened, yet, we do not seek confrontation.

Let me be clear: As secretary, I am committed to pursuing a constructive, stable relationship with China, including stronger crisis communications with the People's Liberation Army. You know, big powers need to model transparency and communication. We hope that we can work together with Beijing on common challenges, especially the threat of climate change. Even in times of competition, our enduring ties in Southeast Asia are bigger than just geopolitics. As Singaporean Prime Minister Lee Hsien Loong has counseled, we are not asking countries in the region to choose between the United States and China. In fact, many of our partnerships in the region are older than the People's Republic of China itself.

That's why we are expanding our important work with countries throughout the Indo-Pacific and with ASEAN itself, a critical body that brings the region closer together, offering everyone a voice and building deeper habits of cooperation.

I'll say personally that I'm proud that my predecessors and I have attended every single meeting of the ASEAN Defense Ministers Meeting-Plus, a venue that is increasingly central to the region's security architecture. ASEAN is also showing its ability to lead on the region's most important issues. We applaud ASEAN for its efforts to end the tragic violence in Myanmar. The Myanmar

military's refusal to respect the inalienable rights of the Burmese people and to defend their basic well-being is flatly unacceptable. A military exists to serve its people — not the other way around. We call on the Myanmar military to adhere to the ASEAN Five-Point Consensus and to forge a lasting peace.

As ASEAN plays its central role, we are also focusing on complementary mechanisms in the region. I know how pleased President Biden was to host the first Quad Leaders' Summit in March 2021. Structures like the Quad make the region's security architecture even more durable. We're also taking a leading role again at the U.N. Security Council. That includes enforcing its critical resolutions about nuclear dangers on the Korean Peninsula. We're taking a calibrated, practical approach that leaves the door open to diplomacy with North Korea, even while we maintain our readiness to deter aggression and to uphold our treaty commitments and the will of the Security Council.

Our partnerships draw strength from our shared belief in greater openness, and our belief that people live best when they govern themselves. Now, our democratic values aren't always easy to reach. And the United States doesn't always get it right. We've seen some painful lapses, like the unacceptable and frankly un-American discrimination that some Asian Americans and Pacific Islanders have endured in my country in recent months.

I believe that we're better than that — far better. But we aren't trying to hide our mistakes. When a democracy stumbles, everyone can see and hear it. It's broadcast in loud and living color and not hushed up by the state.

Our openness gives us the built-in ability to self-correct and to strive toward a more perfect union. When we come up short, when we stray from our Constitution's wisdom, we have a pretty good track record of owning up and trying to do better. Even in times of challenge, our democracy is a powerful engine for its own renewal. We've embarked upon an ambitious program to "build back better" after the pandemic. President Biden likes to tell the world leaders he meets with that it's "never, ever, ever been a good bet to bet against America."

What ties all of this together is one simple insight: When we work hand in hand with our friends, we are stronger and more secure than we could ever be on our own. And that's what guides my approach to this most important region as secretary of defense.

Our alliances are an unmatched and unrivaled source of strength and security. As a fellow Indo-Pacific country, we believe that the next chapter in the story of this region can be an inspiring one, a time where, as President Biden likes to say, hope and history rhyme.

We stand together with you, as your allies, your partners and your friends, because we know that no one can go it alone. We are confident that together, we can build a better and brighter future for all of our children. □

This version of Austin's speech has been edited to fit FORUM's format.

HOLISTIC APPROACH



'INTEGRATED DETERRENCE' KEY TO INDO-PACIFIC PEACE

FORUM STAFF

When North Korea tested ballistic missiles seven times in less than a month in January 2022, it violated several United Nations Security Council resolutions. Pyongyang kicked off the record month of testing by launching a hypersonic missile capable of maneuvering at high speeds, and it followed that up with a flurry of ballistic missile launches into the Sea of Japan.

North Korea's self-ascribed deterrent programs, coupled with the snowballing military buildup of the Chinese Communist Party, have the United States and its allies doubling their deterrence efforts. In an age of hypersonic weapons that can travel at five times the speed of sound and long-range missiles that can change trajectory, today's threats require what U.S. Secretary of Defense Lloyd Austin calls "integrated deterrence," a security approach tailored to the region's landscape with a partnership of allies and friends working together.

"The cornerstone of America's defense is still deterrence, ensuring that our adversaries understand the folly of outright conflict," Austin said in an April 2021 change-of-command ceremony at U.S. Indo-Pacific Command in Hawaii. "Throughout American history, deterrence has meant fixing a basic truth within the minds of our potential foes: And that truth is that the costs and risks of aggression are out of line with any conceivable benefit."

Going forward, that deterrence philosophy must be highly integrated across all services and domains and with allies and partners, Austin said. Nowhere is this integrated deterrence philosophy more apparent than in the Indo-Pacific, where the U.S. and its allies are working together on everything from small satellites to nuclear submarine technology to deter potential adversaries.

INTEGRATED MISSILE DEFENSE

A Patriot surface-to-air missile pierced the skies over Queensland, Australia, in July 2021, marking the

A Patriot missile launches from Australian soil for the first time during Talisman Sabre 21, a large-scale multilateral exercise in July 2021. MAJ. TREVOR WILD/U.S. ARMY



The United States works with allies and partners to deter potential adversaries during the Rim of the Pacific exercise, held off the coast of Hawaii in 2020. Participants included Australia, Brunei, Canada, France, Japan, New Zealand, the Philippines, Singapore and South Korea.

PETTY OFFICER 3RD CLASS JENNA DO/U.S. NAVY

first time the technology had been used in Australia and signaling the type of deterrence the U.S. is trying to achieve. U.S. Soldiers from the 38th Air Defense Artillery Brigade, 94th Army Air and Missile Defense Command, destroyed two unmanned aerial vehicles with Patriot missiles while operating with Australian Defence Force personnel during exercise Talisman Sabre 21, which involved more than 17,000 participants from seven nations.

In addition to demonstrating how U.S. forces can rapidly deploy anywhere in the region, the exercise showed a technological integration the allies believe is key in 21st century warfare. "We successfully demonstrated that we can operate with Australian weapons systems, that we can coordinate communications and engage targets in the sky together," U.S. Army Capt. Phillip Le, commander of Alpha Battery, said in a news release.

The historic Australia launch was "just tremendous and a real privilege to see in action," said Maj. Gen. Jake Ellwood, commander of Australia's Deployable Joint Force Headquarters, according to

Australian Security Magazine. The MIM-104 Patriot missile can travel at about 1,715 meters per second and strike targets that include aircraft and ballistic and cruise missiles.

Such military exercises involving the U.S. and its Indo-Pacific partners hone technological expertise and generate “signaling” value to potential adversaries, Bruce W. Bennett, a defense analyst with the Rand Corp., told FORUM. “North Korea in particular would love to see the Republic of Korea-U.S. alliance broken,” Bennett said. “That’s one of their key objectives — to break the alliance if they can. And they’re doing a lot of work to that end. China would also be happy to see U.S. alliances in the region broken. China is trying to establish a degree of leverage or, eventually, dominance over all of its neighbors.”

By sharing technology with its regional partners, the U.S. is offering an alternative that involves partnership rather than subjugation, he said. “The U.S. isn’t trying to dominate those alliances,” Bennett said. “Instead, it’s giving out its most modern technology in many cases to its allies. The U.S. is simply trying to make it clear that in a world where China would like to dominate, Washington is trying to maintain an ability to provide an alternative to Chinese dominance and maintain a good relationship with the regional countries without trying to double the U.S. defense budget.”

STRONGER THROUGH INTEGRATION

Integrated deterrence isn’t only about signaling, however. It’s about mission success. Bennett offered the hypothetical example of North Korea firing one of its Nodong intermediate-range ballistic missiles into South Korea. “If you’ve got a radar for a Patriot interceptor that’s looking at the missile coming in, it’s looking down the barrel of the gun, so to speak,” Bennett said. “It’s relatively hard to tell the exact

trajectory and that sort of thing. But if that radar is keyed to a radar sitting in Japan, looking at the trajectory from the side, it is far easier to determine exactly what maneuvers or what the trajectory itself looks like because you’re getting both the ‘down the barrel’ and ‘from the side’ perspectives. And that makes it a lot easier to be effective in intercepting it.”

If Australia, Japan, South Korea and the U.S. operate radars in concert, there is a cost-sharing benefit, too, Bennett said.

NEWLY INTEGRATED FRONTIER

When Austin talks about integrated deterrence, he points out that integration needs to occur across services, with allies and partners and beyond the traditional domains of air, land and sea. Space and cyberspace are where 21st century conflicts could begin, and partnerships in those domains are critical for detecting and deterring attacks.

To that end, Japan and the U.S. plan to collaborate on the deployment of a network of small satellites in low Earth orbit to detect and track next-generation missiles, the Nikkei Asia website reported in August 2020. The U.S. \$9 billion project is expected to be operational by the mid-2020s. The evolving nature of the region’s missile threat requires more space-based sensors, the article concluded. The PRC possesses about 2,000 medium-range missiles capable of striking Japan, according to the Nikkei report, and it has hundreds of nuclear warheads. North Korea has hundreds of medium-range missiles and continues in its quest to miniaturize nuclear warheads. These missiles fly in parabolic trajectories, which makes them easier to track and intercept with satellites and radar systems operated by Japan and the U.S.

The U.S. Navy’s USS Key West is a nuclear-powered, fast-attack submarine. The United States and the United Kingdom will share their nuclear propulsion technology with Australia in a new strategic partnership. PETTY OFFICER 1ST CLASS JEFFREY JAY PRICE/U.S. NAVY



North Korea, the People's Republic of China (PRC), and Russia, however, are developing weapons designed to evade these shields. The PRC and Russia are testing hypersonic missiles, which fly at more than five times the speed of sound and at low altitudes, and North Korea is experimenting with long-range missiles that can change trajectory.

The ballistic missiles North Korea fired into the Sea of Japan in September 2021 flew at low altitudes and irregular trajectories, making them difficult to intercept, according to a report by Jiji Press. "It's clear that the missiles were designed to evade missile defense systems of Japan and the United States," an official at Japan's Defense Ministry said, according to the report.

The existing satellite network employed by Japan and the U.S. operates at altitudes of 36,000 kilometers, Nikkei reported. To address the gap, the U.S. plans to launch satellites at altitudes between 300 kilometers and 1,000 kilometers. The plan is for 1,000 miniature observation satellites, with 200 equipped with heat-detecting infrared sensors designed for missile defense.

HISTORIC MULTIDIMENSIONAL PACT

In another historic move, the United Kingdom and the U.S. announced in September 2021 that they would help Australia acquire nuclear-powered submarines as part of a trilateral security partnership. Known as AUKUS, the partnership will establish channels of information sharing and foster joint efforts to develop advanced technologies in cybersecurity, artificial intelligence, quantum computing and undersea capabilities, the news website Axios reported.

Teams from the three countries will work for 18 months to identify the best way to deliver nuclear-powered submarines to Australia. The U.S. had previously only shared its nuclear submarine technology with the U.K.

U.S. President Joe Biden heralded the pact as strategically necessary. "Our nations and our brave fighting forces have stood shoulder to shoulder for literally more than 100 years, through the trench-fighting in World War I, the island-hopping in World War II, during the frigid winters in Korea and the scorching heat in the Persian Gulf," President Biden said at a news conference, flanked virtually by U.K. Prime Minister Boris Johnson and Australian Prime Minister Scott Morrison. "Today we take another historic step to deepen and formalize cooperation among all three of our nations. Because we all recognize the imperative of ensuring peace and stability in the Indo-Pacific over the long term," he said.

In briefing reporters, U.S. officials said the nuclear propulsion technology being shared will



A Japanese satellite deploys outside the International Space Station. Japan and the United States plan to work together to produce a constellation of small satellites that could detect missile attacks. NASA

allow Australia to deploy quieter and more capable submarines for longer periods. Australia does not seek nuclear weapons, the officials said.

Bennett explained that geography plays a key role in the decision. Diesel submarines create toxic exhaust that must be evacuated from the vessel periodically, so diesel subs must "snorkel" or surface to do that. "If the Japanese or South Korean submarines have diesel technology, well, they've got lots of islands that they can go to in their territorial waters and snorkel or surface, and then go back underwater and disappear," Bennett said. "But if a submarine from Australia is trying to get up to Japan or South Korea, it has to transit a very long distance in front of the east coast of China. And as China's surveillance technology gets better, China's potentially able to detect those submarines and potentially intercept them. Today it's probably not such a big deal. But in 20 years, which is roughly when the nuclear submarines for Australia will become available, it probably will be a very big deal."

From missile technology to nuclear propulsion, the U.S. is demonstrating its commitment to a Free and Open Indo-Pacific. The integrated deterrence approach relies not only on technology sharing but also intelligence and information sharing. That, defense officials said, may require economic and diplomatic efforts in some instances. "If we are really going to deter countries that are rising as fast as China, or are getting as assertive and aggressive as Russia, we're going to need friends," Colin Kahl, U.S. undersecretary of defense for policy, told colleagues during a June 2021 meeting at the Pentagon, according to Department of Defense News. "We're going to need to integrate them into our understanding of what deterrence means." □



TRUTHS UNKNOWN

FORUM ILLUSTRATION

Inability to verify North Korean claims prompts questions about the status of its people, missiles, leadership

FORUM STAFF

Transparency in international relations is critical to building trust and avoiding conflict. However, North Korea's regime has remained anything but forthright when it comes to disclosing confirmable information about the welfare of its people, efforts to denuclearize or the lack thereof, and the health — and often location — of its leader.

The inability of the international community to verify North Korea's claims of zero COVID-19 cases and the increase in frequency and duration of dictator Kim Jong Un's disappearances from the public in 2020 and 2021 add to speculation over the regime's instability.

"Still, it never pays to sell the regime short. It has outlived countless previous reports of its imminent demise," Bruce Klingner, senior research fellow for Northeast Asia at The Heritage Foundation, wrote for the think tank's website in July 2021.

Indeed, even as Kim reemerged in June 2021 looking thinner after a four-week hiatus and prompting more conjecture about his health, the regime would resume its provocations three months later by testing a series of missile systems just days apart, in violation of several United Nations Security Council resolutions. If there were any question about the future of the Kim dynasty should rumors of the current ruler's failing health be true, then Kim's younger sister, Kim Yo Jong, has been positioned as a possible answer.

"Since representing Kim [Jong Un] at the 2018 Winter Olympics in Pyeongchang, South Korea, Kim Yo Jong has not only acquired prestigious titles within the ruling Workers' Party. . . she enjoys the absolute confidence of her brother, a leader capable of ordering the execution of his own uncle for alleged treason," according to The Guardian newspaper.

Kim Yo Jong remains at her brother's side during key events. Rising to prominence in recent years, she attended each of the three face-to-face meetings between Kim Jong Un and then-United States President Donald Trump, according to The Wall Street Journal newspaper. The Journal credits Kim Yo Jong with leading North Korea's propaganda and agitation department and signing off on a North Korean statement criticizing the U.S. in 2020 for its insistence that the country denuclearize and a statement rebuking South Korea for criticizing a military exercise by the North.

She again gained media attention in September

2021 by warning of "complete destruction" of bilateral ties with South Korea if then-South Korean President Moon Jae-in continued to describe the North's weapons demonstrations as provocation, The Associated Press (AP) reported.

"If the president joins in the slander and detraction (against us), this will be followed by counter actions, and the North-South relations will be pushed toward a complete destruction," her statement said, according to AP. "We do not want that."



Kim Yo Jong, the younger sister of North Korean dictator Kim Jong Un, has seen her prominence rise within the regime. THE ASSOCIATED PRESS

Three Kim men have ruled North Korea since 1948, starting with Kim Il Sung, followed by his son, Kim Jong Il, and then his grandson, Kim Jong Un. Kim Yo Jong's status may be rising, but experts say there's no concrete evidence that she would ever become the next regime leader. In fact, most analysts say don't count down the days of Kim Jong Un's rule just yet. Some opine that his more-slender frame could be an attempt to improve his health and longevity rather than signs of sickness, according to AP.

STILL AT WAR

North and South Korea technically remain at war because the 1950-53 Korean War ended in an armistice and not a peace treaty. Attempts at reunification have failed, but in September 2021, Moon again called for an official end to the war.

"Today, I once again urge the community of nations to mobilize its strengths for the end-of-war declaration on the Korean Peninsula and propose that three parties of the two Koreas and the U.S., or four parties



Then-South Korean President Moon Jae-in, second from left, greets North Korean leader Kim Jong Un's sister, Kim Yo Jong, ahead of an inter-Korean Summit in April 2018 in South Korea. GETTY IMAGES

of the two Koreas, the U.S. and China, come together and declare that the war on the Korean Peninsula is over," Moon told the U.N. General Assembly.

The most ardent dream of the global community, he said, "is creating a life that is peaceful and secure." Such a dream remains unrealized on the peninsula, despite efforts by the U.N. and others, he said. South Korea, however, remains committed to ensuring lasting peace takes "firm root" on the peninsula, he said.

"Envisioning a denuclearized, co-prosperous Korean Peninsula, the government of the Republic of Korea [South Korea] has steadily carried forward the Korean Peninsula peace process, and amid the support of the international community, achieved historic milestones," Moon said. "Peace on the Korean Peninsula begins always with dialogue and cooperation. I call for speedy resumption of dialogue between the two Koreas and between the United States and North Korea."

Kim Yo Jong responded by calling on the South to abandon "hostile policies" and "double-dealing standards" if it wants to take steps toward reconciliation, according to AP. She did not elaborate, but experts suspect North Korea wants South Korea to help it win relief from sanctions and receive other concessions that might include international recognition as a nuclear weapons state, according to AP.

"I think that only when impartiality and the attitude of respecting each other are maintained, can there be

smooth understanding between the North and the South," Kim Yo Jong said, according to CNN. "I felt that the atmosphere of the South Korean public desire to recover the inter-Korean relations from a deadlock and achieve peaceful stability as soon as possible is irresistibly strong. We, too, have the same desire."

Lee Sung-yoon, a North Korea expert at The Fletcher School at Tufts University, cautioned that Kim Yo Jong might merely be dangling everything "Moon desperately desires before his term expires" in May 2022, according to The New York Times newspaper. Kim Yo Jong "shows once again how adept she is in the art of psychological manipulation," Lee told the Times.

Kim Yo Jong called her statement "just my opinion," according to the Times. Nevertheless, South Korea acknowledged it as meaningful. Still, actions speak louder than words, and South Korea's Unification Ministry noted the inconsistency in North Korea's willingness to communicate. The regime had stopped taking South Korea's calls on a hotline to manage bilateral military relations in August 2021 before restoring communication again two months later.

"It is more important than anything else to have communication in a smooth and stable manner so as to realize denuclearization, the establishment of lasting peace on the Korean Peninsula, and the advancement of relations between the South and the North through dialogue and cooperation," Lee Jong-joo, the ministry's spokeswoman, told reporters in late September 2021.

CHANGES APPARENT

Kim Jong Un's weight loss isn't the only change providing analyst talking points. Spectators expected a grand show during a North Korean military parade in September 2021. Instead, a toned-down event took place, reflecting what experts see as a harsh reality of a broken North Korea. The country has struggled, they said, due to prolonged border closures because of the pandemic, food shortages from flooding, sanctions and a mismanaged economy. Kim also did not deliver an address.

"North Korean society is under tremendous stress because of decisions made by the Kim regime. So, the parade is intended to show strength and serve as a quarantine morale booster," Leif-Eric Easley, a professor of international studies at Ewha Womans University in Seoul, told the Times before warning, "We shouldn't over-interpret foreign policy or negotiating signals from a parade that's primarily aimed at domestic political audiences."

Seen largely as an attempt to generate national unity, the September parade took place amid North Korea's worst food crisis in a decade, according to a U.N. Food and Agriculture Organization report. More astonishing, however, was Kim's public acknowledgment of the crisis in June 2021, when he said resolving the food shortage was "a top priority."

"In particular, the people's food situation is now getting tense as the agriculture sector failed to fulfill its grain production" after flood damage, he said, according to the Times. "It is essential for the whole party and state to concentrate on farming."

As North Korea prolonged border closures — even with China — because of the pandemic, essential items such as medicines have become harder to obtain, the Times reported. More homeless children are scouring trash bins for food in parts of the country, and families are selling furniture to buy food, the Times reported.

"When he [Kim] took power a decade ago, one of his first promises was to ensure that his long-suffering people would 'no longer have to tighten their belt.' But those economic plans suffered a setback when the country's growing weapons arsenal led to punishing international sanctions," the newspaper reported.

The North Korean regime rarely confirms anything negative or potentially nefarious happening within its borders. What Kim and his Workers' Party won't reveal, satellites will.

For example, satellite imagery in August 2021 revealed that North Korea appeared to have restarted the plutonium-producing reactor at its Yongbyon nuclear research facility, according to the International Atomic Energy Agency (IAEA), which uses imagery and open-source material to monitor North Korea's activities. Then imagery in September 2021 exposed that renovations were underway at the Yongbyon

complex that could allow North Korea to increase its production of weapons-grade nuclear material by as much as 25%, Jeffrey Lewis, a weapons expert and professor at the Middlebury Institute of International Studies, told CNN. "The most recent expansion at Yongbyon probably reflects plans to increase production of nuclear materials for weapons production," he said.

Lewis noted the construction is consistent with ongoing work to add floorspace at the facility. The new area — approximately 1,000 square meters — could house as many as 1,000 additional centrifuges, making it possible to enrich more uranium annually, he told CNN.

As evidence mounts of North Korea's continued nuclear ambitions, the U.S. has remained steadfast in attempts to achieve denuclearization diplomatically. "We have been very clear about what we want to see happen," U.S. State Department spokesman Ned Price said, according to CNN. "We are committed to the principle that dialogue will allow us to pursue our ultimate objective, and that's quite simply the denuclearization of the Korean Peninsula."



Moon Jae-in addresses the 76th session of the United Nations General Assembly in September 2021, where he pushed for a declaration to formally end the 1950-53 Korean War to restore peace on the Korean Peninsula. THE ASSOCIATED PRESS

Using its official name of the Democratic People's Republic of Korea (DPRK), IAEA Director General Rafael Mariano Grossi described North Korea's nuclear activities as "cause for serious concern" and "deeply troubling."

"The continuation of the DPRK's nuclear program is a clear violation of relevant U.N. Security Council resolutions and is deeply regrettable," Grossi said in September 2021 during his IAEA General Conference speech. "I call upon the DPRK to comply fully with

its obligations under relevant U.N. Security Council resolutions, to cooperate promptly with the agency in the full and effective implementation of its NPT [Non-Proliferation Treaty] Safeguards Agreement and to resolve all outstanding issues, especially those that have arisen during the absence of agency inspectors from the country.”

Analysts also point to the uptick in ballistic missile tests conducted at the start of 2022 by North Korea as a sign of Kim’s continued defiance of international law and stockpiling of materials for weapons of mass destruction (WMD). North Korea conducted seven ballistic missile tests in January 2022, more than in all of 2021, prompting the U.S. to levy a new round of sanctions against individuals and entities accused of helping develop and procure ballistic missile-related materials for Kim.



Visitors look toward North Korea from South Korea’s Odusan observatory near the Demilitarized Zone separating the two Koreas. AFP/GETTY IMAGES

Kim continued to escalate tensions in early 2022, conducting tests February 27 and March 5 of what U.S. administration officials characterized as “a relatively new intercontinental ballistic missile system,” which triggered additional U.S. sanctions. A 10th test March 16 ended in apparent failure, exploding soon after liftoff, according to South Korean reports, but fueled speculation that larger tests would be forthcoming.

After the February test, the U.S. and 10 other countries condemned the ballistic missile launch as “unlawful and destabilizing” and urged the U.N. Security Council to condemn the North Korean regime for violating multiple council resolutions. U.S. Deputy Ambassador Jeffrey DeLaurentis read

the 11 U.N. members’ joint statement surrounded by diplomats from six other council nations — Albania, Brazil, France, Ireland, Norway and the United Kingdom — as well as Australia, Japan, New Zealand and South Korea. “We remain committed to seeking serious and sustained diplomacy and urge Pyongyang to respond positively to outreach from the United States and others,” the statement said. The 11 countries urged North Korea “to choose the path of diplomacy to ease regional tensions and promote international peace and security” and affirmed their readiness for dialogue, stressing that “we will not waver in our pursuit of peace and stability.”

HUMAN RIGHTS

Unyielding international sanctions and a persisting pandemic have exacerbated the daily hardships inflicted by the regime on North Korean citizens. Through it all, labor camps continue to exist. Nongovernmental organizations (NGOs) and others charge that these camps violate human rights. Meanwhile, Kim Jong Un in September 2021 thanked the youth for “volunteering” for mandatory labor to atone for “lagging behind” or “cultural infiltration,” according to Human Rights Watch, an international NGO headquartered in New York City.

“The North Korean government’s use of hard labor justified by ideological demands is common. The demanded labor is used for projects that Kim Jong Un has deemed a priority, such as mining, farming and construction,” according to Human Rights Watch. “This allows North Korea to boost domestic production — even more relevant now that cross-border trade has almost stopped — while sending specific political messages to the people.”

In April 2021, Kim ordered a crackdown on things the regime considers anti-socialist, individualistic or unsavory. Those included words, acts and fashion.

“Young people were directed to stop watching, reading or listening to unsanctioned videos, broadcasts or texts; not mimic the speech, clothes and hairstyles of South Korean television series characters; and re-embrace a life that shows loyalty to the North Korean leadership, carries on the socialist system and follows the government’s propaganda and orders,” Human Rights Watch reported. “These so-called ‘volunteer’ mobilizations of people to work in mines, farms or construction sites involve backbreaking labor under extremely harsh and dangerous conditions for long periods of time with little or no pay. The North Korean government may say these are all volunteer projects, but the reality is very few people can turn down the request. Since punishment for crimes in North Korea is arbitrary, depending on a person’s record of loyalty, personal connections, and capacity to pay bribes, refusal to work as a ‘volunteer’ can result



A slimmer Kim Jong Un attends a paramilitary parade marking the 73rd anniversary of the republic at Kim Il Sung square in Pyongyang in September 2021. THE ASSOCIATED PRESS

in severe punishment, including torture and long imprisonment.”

The U.N. Human Rights Council monitors North Korean prison camps, seeking to interview survivors who escape and pledging to prosecute Kim Jong Un and other North Korean officials engaged in abuses.

“Analysis of available information continues to confirm that there are reasonable grounds to believe that crimes against humanity have been committed and may be ongoing in the Democratic People’s Republic of Korea,” the U.N.’s Office of the High Commissioner for Human Rights (OHCHR) reported in January 2021. “OHCHR reiterates that there is no statute of limitations for crimes against humanity, and that those responsible for past and ongoing crimes should be held accountable. A lasting peace on the Korean Peninsula can be achieved only if such violations end and the rights of victims to truth, justice, reparations and guarantees of non-recurrence are fulfilled.”

Ahn Myeong Chul knows the atrocities occurring inside the walls of North Korean prison camps all too well. A former Korean People’s Army soldier, Ahn worked as a guard at various prison camps, including the Hoeryong and Onsong concentration camps, from the 1980s to the 1990s. He escaped and fled to South Korea. Now, Ahn is executive director of NK Watch, a Seoul-based NGO devoted to assisting North Korean defectors and bringing Kim Jong Un to trial at the International Criminal Court in The Hague,

Netherlands, for crimes against humanity.

“The problem of forced labor or deficient food distribution in North Korea has been happening continuously for 70 years since the birth of the North Korean government. The overall situation of human rights in North Korea is very poor,” Ahn told FORUM. “The biggest reason for this is that the Kim family blocks information about the outside world in order to maintain their system, and North Koreans have been exposed only to the propaganda of idolization of the Kim family since their childhood, so they know nothing about the outside world. As a result, there is an atmosphere among North Korean residents of accepting that they are born to live in such ways.”

Ahn said defectors help bring some change to the closed society, delivering outside news through phone calls and other means. More must be done, he said, imploring the international community to keep human rights atrocities at the forefront of conversations about North Korea as much as discussions on denuclearization.

Many truths, moreover, are known within the country’s borders. “North Korea’s biggest Achilles’ heel is the human rights issue,” Ahn told FORUM. “I can’t express it in words, but North Korean people are being tortured. The international community must continue to send the message to North Korea that crimes against humanity must be punished internationally.” □

A DANGEROUS FRONTIER



U.S. Space Command Adapts to Increasingly Complex Battleground

BRIG. GEN. DEVIN R. PEPPER/U.S. SPACE COMMAND

The space environment is more competitive and dangerous than ever before. Technological advances, changes in strategic guidance and new security challenges require United States Space Command (USSPACECOM) to adapt and innovate to ensure its space warfighters are prepared to accomplish missions in, from and to space.

Space affects almost every aspect of modern life, from commerce, travel and entertainment to communications and GPS. These activities and functions all rely on space capabilities. Global reliance on space is so extensive that any degradation in capability would significantly impact daily life. Societies around the world expect services provided by these capabilities to be ever present and persistent.

Today, there are over 3,500 operational satellites in orbit. Lower costs and reduced barriers for launch and licensing have thrust the commercial space sector into one of the fastest-growing industries in the world. Commercial firms are now participating in satellite construction, space launch and exploration and even human spaceflight. These firms not only supply products to governments, they also compete in the global economy. The synergy between the civilian sector and the U.S. government has provided for space superiority that enables the joint force to rapidly transition from competition to conflict and prevail in a global, multidomain fight.



Opposite page: A rocket carrying the Tianzhou 3 cargo ship launches from the Wenchang Space Launch Centre on September 20, 2021, on a mission to deliver supplies to China's Tiangong space station. AFP/GETTY IMAGES

The third Space-Based Infrared Systems Geosynchronous Earth Orbit satellite takes off aboard an Atlas V rocket. The U.S. Air Force's 45th Space Wing supported United Launch Alliance's successful liftoff from Cape Canaveral, Florida.

UNITED LAUNCH ALLIANCE



U.S. Navy Lt. Nicole Breen, an intelligence officer, and U.S. Air Force Master Sgt. Kenneth Bangay, a cyber systems operator, are assigned to the National Space Defense Center at Schriever Air Force Base, Colorado.



A crew member at the U.S. National Space Defense Center monitors for space-based threats.

KATHRYN DAMON/U.S. SPACE FORCE

The U.S., along with its allies and partners, faces rapidly growing threats to high-value assets and capabilities in space. The People's Republic of China (PRC) is ruled by a revisionist, communist party that intends to undermine international order and shape the Indo-Pacific region to its advantage. The PRC publicly supports peaceful and responsible uses of space while it simultaneously develops and deploys counterspace weapons designed to hold U.S. and allied space capabilities at risk. The PRC already has operational ground-based anti-satellite missiles, and it tested an orbital hypersonic weapon in July 2021, further increasing tensions in the region and beyond. The growth of adversary counterspace arsenals presents an immediate and serious threat to all peaceful space activities.

USSPACECOM provides space combat power by fully integrating offensive and defensive operations with long-standing allies and partners. USSPACECOM integrates and synchronizes space capabilities and operations as part of the joint and combined force to deter and, if necessary, defeat adversary aggression. The command capitalizes on space domain awareness (SDA) agreements and joint exercises such as Pacific Fury, Pacific Sentry and Talisman Sabre 21 to enhance relationships and operational capability with allies and partners. USSPACECOM is dedicated to allies and partners — building a coalition to defend the space domain from threats — and will continue to participate in joint exercises and SDA agreements globally. Demonstrating its commitment to allies and partners while enhancing interoperability



Soldiers with the U.S. Army's 414th Signal Company, Special Troops Battalion, 3rd Sustainment Brigade, train to use a transportable satellite terminal in Kuwait.

SGT. MARQUIS HOPKINS/U.S. ARMY

sends a strong deterrent signal to adversaries seeking to exploit vulnerabilities.

About 100 personnel from USSPACECOM, the Combined Force Space Component Command, Space Operations Command (SpOC), and Space and Missile Defense Command seamlessly integrated with the Australian Defence Force and Space Operations Center during Exercise Talisman Sabre 21. Objectives included the coordination and orchestration of command and control of space operations as well as control of defensive and offensive space domains.

Exercises such as Talisman Sabre 21, which involved 17,000 personnel from Canada, Japan, New Zealand, the Republic of Korea, the United Kingdom and the U.S., provide effective and practical training to ensure space warfighters and forces are capable, interoperable, deployable on short notice and combat ready. "In modern warfare, multidomain superiority is the lifeblood of effective combined force operations. In Talisman Sabre 21, we took critical steps to promote interoperability and demonstrate the flexibility, responsiveness and relevance of our space forces in

the Indo-Pacific," said Maj. Gen. David N. Miller Jr., USSPACECOM's director of operations, training and force development. "I couldn't be more excited for the future as U.S. Space Command cements our enduring relationship with Indo-Pacific Command and our regional partners to promote security and stability and ensure our combined and joint forces have the space-enabled combat edge they depend upon ... all day, every day."

Talisman Sabre 21, which took place July 14-31, 2021, in Australia, marked the first exercise deployment since USSPACECOM and SpOC established the Counter Communications System, a space electronic warfare system that reversibly denies adversary satellite communication.

The U.S., along with its allies and partners, promotes the responsible use of space. The U.S., other spacefaring nations and the international community consider safe, unfettered access to and freedom to operate in space a vital interest. Should conflict arise, USSPACECOM is ready to support the joint force, while denying any foreign space-related aggression. □

STRATEGIC CHALLENGES



USSTRATCOM Commander: Nuclear-Capable Competitors Pose Complex Threats

FORUM STAFF

FORUM ILLUSTRATION



The U.S. Air Force B-52H Stratofortress, which was deployed to the Indo-Pacific region in support of the Bomber Task Force, provides tactical flexibility to U.S. forces.

MASTER SGT. RICHARD P. EBENSBERGER/
U.S. AIR FORCE

United States Strategic Command (USSTRATCOM) at Offutt Air Force Base near Omaha, Nebraska, combines the U.S. nuclear command and control mission with the global responsibility for strike missions and missile defense. The command is responsible for providing U.S. leadership a greater understanding of threats from around the world and viable means and options to rapidly respond to them.

USSTRATCOM deters strategic attacks and employs forces to guarantee the security of the U.S. and its allies. It is responsible for prevailing in any strategic conflict and for developing the intellectual capital to forge 21st century strategic deterrence.

The command's nerve center is the Global Operations Center, which provides situational awareness and gives the USSTRATCOM commander the mechanism to command and control the nation's strategic forces. FORUM recently interviewed the commander, U.S. Navy Adm. Charles "Chas" A. Richard, and discussed deterrence in an era of strategic competition.

FORUM: *What challenges does the global strategic environment present to deterring aggression and coercion? Can you expound on how security challenges have evolved in the Indo-Pacific region in terms of technologies and weapons systems?*

Adm. Richard: For the first time in our history, the nation is on a trajectory to face two nuclear-capable, strategic peer adversaries at the same time, who must be deterred differently. Today, both China and Russia have the ability to unilaterally escalate a conflict to any level of violence, in any domain and in any geographic location. We have not faced competitors with this ability in over 30 years.

As outlined in the most recent Interim National Security Strategic Guidance, China, in particular, has rapidly become more assertive. They should no longer be viewed as a lesser-included case to Russia but as a pacing nuclear threat. Collectively, China's strategic nuclear modernization expansion raises troubling concerns and complements the conventional capability growth reported by U.S. Indo-Pacific Command (USINDOPACOM) and other combatant commands.



U.S. Navy Adm. Charles "Chas" A. Richard

In addition, over the past decade, Russia has recapitalized roughly 80% of its strategic nuclear forces, strengthening its overall combat potential with an imposing array of modernization efforts and novel weapons programs designed to ensure a retaliatory strike capability by all three triad legs.

The basic deterrence fundamentals against such threats have not changed. We strive to deny any adversary their aim or impose a cost greater than what they seek, such that the benefit of restraint outweighs the perceived benefit of their possible action. These deterrence fundamentals apply from the gray zone throughout the spectrum of conflict that today is neither linear nor predictable. Deterrence operates continuously from peacetime, through the gray zone, worldwide, across all domains and into conflict. It requires integrated planning and resourcing from the entire [U.S. Defense] Department, across the whole of government and in cooperation with allies and partners.

FORUM: *What is USSTRATCOM's role in providing strategic deterrence and maintaining security in the Indo-Pacific region?*

Adm. Richard: U.S. Strategic Command's mission is to deter strategic attacks and employ forces as directed to guarantee the security of the nation and assure our allies and partners. In that role, USSTRATCOM sets the conditions necessary for joint force operations around the world. Every operation plan in the department and every capability assumes that strategic deterrence will hold. None of our plans and no other capability will work as designed if strategic deterrence, and in particular nuclear deterrence, fails.

In addition, the command's capabilities also support the nation's formal extended deterrence commitments that assure European, Asian and Pacific allies and partners. No country should doubt the strength of our extended deterrence commitments or the strength of U.S. and allied capabilities to deter, and if necessary defeat, any potential adversary's nuclear or non-nuclear aggression.

FORUM: *Why are multilateral approaches important for regional security? Do you have a unique approach for China? North Korea? Russia?*

Adm. Richard: Multilateral approaches are important for security as our allies add breadth, depth and resolve. Their resistance to authoritarian visions of the world order strengthens the rules-based international system and magnifies the benefit of restraint among our competitors.

We must maximize our ability to prevent strategic deterrence failure and find ways to reduce the risk of miscalculation in a crisis by engaging all elements of national power to effectively communicate our resolve to potential adversaries. The command stands ready to

support diplomatic efforts as a tool of first resort, using innovative and reliable ways to deter strategic threats and set favorable conditions to shape the global environment.

FORUM: *How would you define 21st century strategic deterrence?*

Adm. Richard: The U.S. Interim National Security Strategic Guidance highlights that, "We must also contend with the reality that the distribution of power across the world is changing, creating new threats." China and Russia are challenging our strength through a wide array of activities that warrant a concerted and integrated whole-of-government response.

This strategic competition demands we be ready for any threat in any domain at any time. Potential adversaries are building advanced nuclear capabilities, fielding increasingly capable conventional forces and exploiting seams below the level of armed conflict in an attempt to gain strategic advantages in pursuit of their national objectives.

The U.S. and our allies and partners must also account for the possibility of conflict leading to conditions which could very rapidly drive an adversary to consider nuclear use as their least bad option.

FORUM: *What must the U.S. do to maintain its strategic advantages in the near and the long terms?*

Adm. Richard: The nation requires a fully modernized nuclear force and supporting infrastructure to ensure the solemn obligation to protect the security of the American people is upheld.

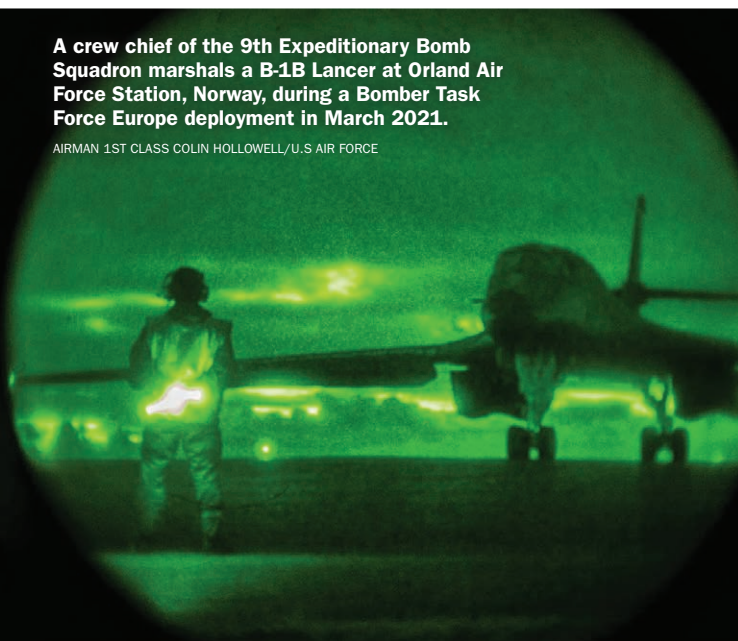
As reaffirmed by every presidential administration over the past 60 years, a safe, secure and effective

A crew chief of the 9th Expeditionary Bomb Squadron marshals a B-1B Lancer at Orland Air Force Station, Norway, during a Bomber Task Force Europe deployment in March 2021.

AIRMAN 1ST CLASS COLIN HOLLOWELL/U.S. AIR FORCE

The ballistic-missile submarine USS Maryland returns to its homeport at Naval Submarine Base Kings Bay, Georgia, following a strategic deterrence patrol.

PETTY OFFICER 2ND CLASS BRYAN TOMFORDE/U.S. NAVY





nuclear force remains the most credible combination of capabilities to deter strategic attack. Current programs of record have been repeatedly shown to be the best way to meet those requirements.

Additionally, our strength is in our ability to work together. Integrating our plans and resources around a commonly defined, threat-based military strategy that includes inputs from across all elements of our national power will posture us against our long-term threat.

FORUM: *How would you describe your priorities for achieving integrated strategic deterrence and for globally integrated operations?*

Adm. Richard: USSTRATCOM will continue to engage with other combatant commanders to integrate planning, operations and activities and highlight the importance of synchronization among all instruments of national power for strategic deterrence.

The importance of our allies in the strategic deterrent equation must not be understated; the threat can manifest in space or cyberspace, and allied participation in developing tailored deterrence achieves our collective security.

FORUM: *How important are submarines to the defense of the Indo-Pacific?*

Adm. Richard: The nuclear triad is made up of three attributes (land-based, sea-based, and air-delivered). The nuclear-powered ballistic missile submarine (SSBN) is the nation's most survivable and enduring nuclear strike platform. The SSBN, which stands for submersible ship, ballistic-nuclear, contributes to deterrence and assurance messaging through partial or full generation of our fleet. With the intercontinental-range Trident II D5 missile, our SSBNs patrol the world's oceans virtually undetected, providing an assured response capability in any scenario.

This assured second-strike capability addresses deterrence gaps in ways unique from other legs of the triad. When paired with its survivability, this crucial capability gives the U.S. president significant latitude for response options.

FORUM: *How do you plan to modernize the land-, sea- and air-based components of strategic deterrence?*

Adm. Richard: USSTRATCOM utilizes capabilities provided by the individual services. The command works with the services to ensure necessary requirements are met when elements of the triad are recapitalized and stands ready to command and control these new weapons systems as they become available.

FORUM: *What are your goals for hypersonic strike technologies? Are we behind our greatest competitors?*

Adm. Richard: Hypersonic weapons show promise to be the conventional complement the nuclear force needs to continue deterring adversaries and offer an opportunity to take further steps to reduce the number of nuclear weapons in our national security strategy. Conventional hypersonic weapons will fill an important role by providing the president with options on holding high-value, time-sensitive and other targets at risk without crossing the nuclear threshold.

Our potential adversaries have dramatically increased their emphasis on weaponization of hypersonic technologies, creating a potential capability gap we must not allow to stand.

Developing and fielding hypersonic weapons has long been a USSTRATCOM requirement and a department priority. They will enable responsive long-range, conventional strike options against distant and defended threats when other forces are unavailable, denied access or not preferred.

FORUM: *What about missile defense?*

Adm. Richard: Missile defense endures as a critical component for comprehensive strategic and tailored regional deterrence.

USSTRATCOM executes its responsibilities for coordinating global missile defense planning and operations support, including advocacy for capabilities and enhancements, and joint training and education in coordination with combatant commands, services and agencies. □

SOLVING A SWARM OF CHALLENGES



A police officer prepares to use a signal-jamming device to disable drones during an anti-terror drill in Seoul, South Korea.

REUTERS

Military, civilian and scientific partners collaborate across Indo-Pacific to counter rising drone threat

FORUM STAFF

The bombs themselves had minimal impact — minor injuries to two Indian Air Force service members and light damage to an air base building in the disputed Jammu and Kashmir region. The mode of delivery, however, reverberated throughout the highest levels of India's military and government and beyond: Small drones dropped the two improvised explosive devices in the late June 2021 attack on the base about 15 kilometers from the India-Pakistan border.

Tagged as the work of terrorists, it was the first attack using bomb-laden drones against an Indian military facility and, according to officials and experts, represented a watershed in asymmetric warfare. With commercial drones readily available and relatively inexpensive, they are a “huge and serious challenge,” retired Indian Army Lt. Gen. D.S. Hooda, who led security efforts in the border region as head of India's Northern Command from 2014-16, told The Associated Press the day of the attack. “Drones have a small visual signature and traditional radars hardly pick them up,” Hooda said. “It will require a whole range of new modifications for the military to intercept and defuse these kinds of attacks.”

It was a prescient warning. Within 24 hours, Indian Soldiers fired on two unmanned aerial vehicles (UAVs) hovering over military areas elsewhere in Jammu and Kashmir, the Hindustan Times newspaper reported. Indian authorities responded swiftly and decisively to the spate of incidents, with measures including heightened investment in counter-drone systems. The initiatives accelerated a whole-of-society approach that mirrors the collaborative efforts underway across the Indo-Pacific region to enlist military, civilian and scientific partners in countering the swarm of challenges posed by drones, whether in the hands of state or nonstate actors. “Drone warfare is one of the most important international security developments of the twenty-first century,” noted a November 2020 essay in Foreign Affairs magazine. “Armed drones are proliferating rapidly, and drone warfare is thus likely to become even more prevalent in coming years.”

In the global trade hub of Singapore, for example, malicious drone activity could devastate the “small, yet congested and complex” airspace, noted an article in Pointer: Journal of the Singapore Armed Forces. The island nation's defense industry has invested in counter-drone technologies “both for commercial and military users seeking to defend their assets from drone threats,” Lt. Col. Ho Sen Kiat, Maj. Lee Mei Yi and Capt. Sim Bao Chen, of the Singapore Armed Forces, wrote in the mid-2018 issue. “This is still an exploratory domain, as many different solutions had been explored internationally, from firing nets from guns or other small drones, to using more advanced technologies like lasers and high-powered microwave.”

HARNESSING NEW TECHNOLOGY

While the Indian military was sifting through the details of the drone attack, Republic of Korea (ROK) special forces were preparing for just such an eventuality in Seoul, South Korea, where the remote-controlled devices have become an increasingly common sight in the skies above the city of 10 million people. During drills at a sports complex in late June, special forces personnel used signal-jamming devices to disable a drone spraying chemicals in a simulated attack. “There are terror attacks using drones happening periodically [around the world] and we have seen appearances of unauthorized drones gradually increasing in Seoul,” Shin Dong-il, a Seoul Metropolitan Police Agency superintendent, told Reuters. “Therefore, we planned this drill as there are growing threats of a new type of terrorism against the city of Seoul, such as terrorism with explosives or chemicals using drones.”

A week earlier, the ROK military unveiled a pilot program for a detection-and-jamming system to stop drones approaching its facilities, reported Yonhap, South Korea's government-affiliated news agency. Developed with indigenous technologies, the radar system can detect drones as small as a baseball up to 8 kilometers away and incapacitate unauthorized

UAVs with signal jammers, according to the nation's Defense Acquisition Program Administration. The announcement soon was followed by news that the ROK military was expediting its acquisition process to speed deployment of artificial intelligence (AI)-based systems and other evolving capabilities, including those related to drones. "As our neighboring countries are putting national efforts toward science and technology development to prepare for the future, our military should also swiftly adopt cutting-edge technologies, such as AI and unmanned systems, and focus on developing defense policies and strategies for the future," South Korean Defense Minister Suh Wook said in late July 2021, according to Yonhap.

“For states that seek to break long-standing geopolitical deadlocks, the rise of relatively cheap, disposable, armed drones offers a tempting opportunity.”

— Jason Lyall

A military technology expert at Dartmouth College in the U.S.

That same month, India's Air Force solicited proposals for 10 anti-drone systems to be deployed at air bases, the Asian News International news agency reported. It called for a domestically developed system that uses a laser-based, directed-energy weapon and can be mounted on vehicles, buildings or open ground. Such weapons could blunt the "potentially transformative threat of drone swarms," according to Jacob Parakilas, a foreign policy and international security analyst. The ability of lasers "to fire for an extended period without drawing down a limited stock of ammunition gives them singular potential against swarms of lightweight drones, which might confound traditional defensive measures," Parakilas wrote in the online magazine *The Diplomat* in September 2021. "In that context, they might well provide a crucial part of a layered defensive system, with electronic defenses, decoys, missiles, and guns all providing countermeasures against different types of threats."

CHINA DRIVING PROLIFERATION

Those threats are escalating. A decade ago, only Israel, the United Kingdom and the United States possessed armed drones, according to research by three U.S.-based academics. Since then, at least 18 countries have joined that group, and "non-democracies became significantly more likely to pursue and obtain armed drones from 2011-2019 due to China's entrance into the drone export market," Michael C. Horowitz and Joshua A. Schwartz of the University of Pennsylvania and Matthew Fuhrmann of Texas A&M University wrote in "Who's Prone to Drone? A Global Time-Series Analysis of Armed Uninhabited Aerial Vehicle Proliferation," published in the journal *Conflict Management and Peace Science* in late 2020.

Unlike Indo-Pacific democracies such as Australia, India, Japan, New Zealand, South Korea and the U.S., the People's Republic of China (PRC) is not among the 35 member nations of the Missile Technology Control Regime, an informal grouping dating to the late 1980s that seeks to limit the spread of missiles and missile technology by controlling exports of related equipment and systems, including drones. Indeed, 11 of the nations that acquired armed drones since 2011 did so from the PRC, according to the research paper, including authoritarian regimes "that violate human rights" and that may use drones to further monitor and repress their citizens. "The spread of drones — and especially armed drones — has significant consequences for international politics. ... The proliferation of armed drones also has important implications for interstate coercion and escalation dynamics," the researchers noted.

"For states that seek to break long-standing geopolitical deadlocks, the rise of relatively cheap, disposable, armed drones offers a tempting opportunity," Jason Lyall, a military technology expert at Dartmouth College in the U.S., noted in the article "The future of drone warfare," published in *The Week* magazine in June 2021. Even unarmed drones can threaten military and security operations when used for surveillance, as decoys or to jam air defense systems. "Armed with relatively inexpensive and unsophisticated equipment, a small drone could gather critical intelligence and provide targeting to other platforms and munitions that could cause much more damage than the drone could itself," noted a July 2021 article in the online magazine *The War Zone*.

In India's case, at least for now, the looming drone threat comes less from enemy nations than from extremist groups and other nonstate combatants. Indian security forces in western regions bordering Pakistan reported about 250 drone sightings from 2019 to 2020, with the UAVs used to deliver



Republic of Korea Soldiers and firefighters inspect a drone during a June 2021 drill in Seoul to prepare for potential terror attacks involving unmanned aerial vehicles armed with explosives or chemical weapons. REUTERS

weapons to terrorists, smuggle drugs and conduct surveillance, according to a June 2021 article in *The Diplomat*. The security environment is increasingly complicated because improved technology has made building drones something akin to a “DIY project that could be tackled at home,” said Indian Army chief Gen. Manoj Mukund Naravane, according to the *Hindustan Times*.

India’s eastern neighbor is grappling with a similar dilemma. In late August 2021, Bangladeshi counterterrorism police announced the arrest of three militants suspected of planning a drone attack on government facilities, the first such threat in the nation of 165 million people, *BenarNews* reported. “The Islamic State militants in the Middle East used drones to carry out such drone attacks. But in Bangladesh, to date we have not seen any attempt by the militants to carry out attacks using drones,” Ishfaq Ilahi Choudhury, a security analyst and retired Bangladesh Air Force commodore, told the news organization. “I would say the militants’ attempt to carry out attacks with drones is a new dimension. Making or improvising drones has almost become a cottage industry. The students and even a low-level technician can make a drone or increase its weight-carrying capacity.”

PROVING THEIR WORTH

Those concerns are fueling the development of counter-drone technology regionwide, including in the U.S., where projects fusing civilian and military expertise are at the leading edge of progress in the fast-evolving field. In mid-2021, the U.S. Army and U.S. Navy successfully tested counter-drone systems being developed by global defense firms. The U.S. Navy completed a six-week deployment of the DroneSentry-X system aboard its experimental testbed vessel, the M80 Stiletto. The AI-powered system can detect drones up to 2 kilometers away and disrupt them at ranges exceeding 300 meters, according to manufacturer DroneShield, which also is working with the national defense agencies of Australia and the U.K., among other clients. “The demonstration saw the M80 go up against ‘drone swarms’ and what has been described as ‘a wide range of unmanned robotic threats,’” noted a July 2021 article in *The War Zone*. “The combination of the Navy’s one-of-a-kind littoral vessel and an automated anti-drone system highlights the increasingly significant threat that lower-end unmanned systems pose to naval operations and may point to these systems becoming more common aboard surface ships.”

At its Yuma Proving Ground in Arizona, meanwhile, the U.S. Army used the Coyote Block 3 system to defeat a swarm of 10 drones of differing size, range and capability, according to the defense news website Janes. Developed by Raytheon Missiles & Defense, the Coyote uses a nonkinetic warhead and “can be recovered, refurbished and reused without leaving the battlefield.” The U.K. Armed Forces also will test Raytheon-developed anti-UAV technology, the High-Energy Laser Weapon System, the company announced in September 2021. “Directed energy weapons are a key element of our future equipment programs and we intend to become a world-leader in the research, manufacture and implementation of this next-generation technology,” U.K. Minister for Defence Procurement Jeremy Quin said in a statement.

Spurred by the air base attack, the Indian Armed Forces also is exploring the promise of next-gen technology to defeat emerging threats. India’s then top general said in late June 2021 that the nation’s three military branches and Defence Research

and Development Organisation (DRDO) are collaborating with academics and other stakeholders to quicken development of counter-drone technology, the Hindustan Times reported. That includes systems with both signal-jamming, or “soft kill,” and laser-based, or “hard kill,” options, according to DRDO Chairman G Satheesh Reddy. By September, the Indian Navy had signed a contract for just such a system, with the Air Force and Army expected to quickly follow suit. The indigenous system, manufactured by Bharat Electronics Ltd., “can instantly detect and jam micro drones and use a laser-based kill mechanism to terminate targets,” according to a joint statement. “It will be an effective, all-encompassing counter to the increased drone threat to strategic naval installations.”

FORCE FOR GOOD, ILL

In many ways, India’s experiences in mid-2021 encapsulate the Jekyll-and-Hyde duality of drones — their capacity to contribute to the common good and their potential, in the wrong hands, to wreak havoc.



The U.S. Army’s Joint Counter-small Unmanned Aircraft Systems Office conducted a weeklong demonstration of emerging counter-drone technology at the Yuma Proving Ground in Arizona in April 2021. MARK SCHAUER/U.S. ARMY

Barely two months after the Jammu and Kashmir attack, the Indian government unveiled streamlined certification requirements and special travel corridors to boost drone use for such activities as agriculture, emergency response, geospatial mapping, infrastructure, law enforcement, surveillance and transportation. “India has the potential to be a global drone hub by 2030 as drones offer tremendous benefits to all sectors of the economy and can be significant creators of employment and economic growth due to their reach, versatility, and ease of use,” India’s Ministry of Civil Aviation said in an August 2021 statement.

Evidence of such benefits can already be seen. In Telangana, India, the government is working with a local startup on a drone-based project to plant 5 million trees across 12,000 hectares of the state. In another public-private collaboration, Telangana is pioneering the use of drones to deliver vaccines, blood and other medical supplies to rural residents through its Medicine from the Sky program, *The Hindu* newspaper reported in September 2021. Similar projects are gathering pace across the region, including in Indonesia, where amateur drone operators spearheaded an innovative program to provide contactless medicine and food delivery to self-isolating COVID-19 patients on remote islands.

The same consumer gadgetry that allows drone hobbyists to save lives also enables extremists to take lives, however. Solving that conundrum is a pressing priority for Indo-Pacific allies and partners. “Technology trends are dramatically transforming legitimate applications of sUAS [small unmanned aircraft systems] while simultaneously making them increasingly capable weapons in the hands of state actors, non-state actors, and criminals,” the U.S. Department of Defense noted in its Counter-Small Unmanned Aircraft Systems Strategy, published in January 2021.

A year earlier, the U.S. Army established its Joint Counter-small Unmanned Aircraft Systems Office (JCO) to lead development of the training, materiel and doctrine required to counter small drones, which “represent a rapidly proliferating, low cost, high-reward and potentially lethal and damaging capability against U.S. personnel, critical assets and interests.” The JCO’s tasks include establishing testing protocols and standards, creating training modules and hosting demonstrations of emerging counter-drone technologies at the Yuma Proving Ground. Some of the tested systems fire a net or rope from an onboard air pistol to entangle an enemy drone’s rotors, while others shoot down drones or ram them midair, according to a U.S. Army news release. “I don’t think there is any question that there is value — we need to have a place for industry to come in and show their technology to counter

the threats to our warfighters,” said Stanley Darbro, deputy director of the U.S. Army’s Rapid Capabilities and Critical Technologies Office.

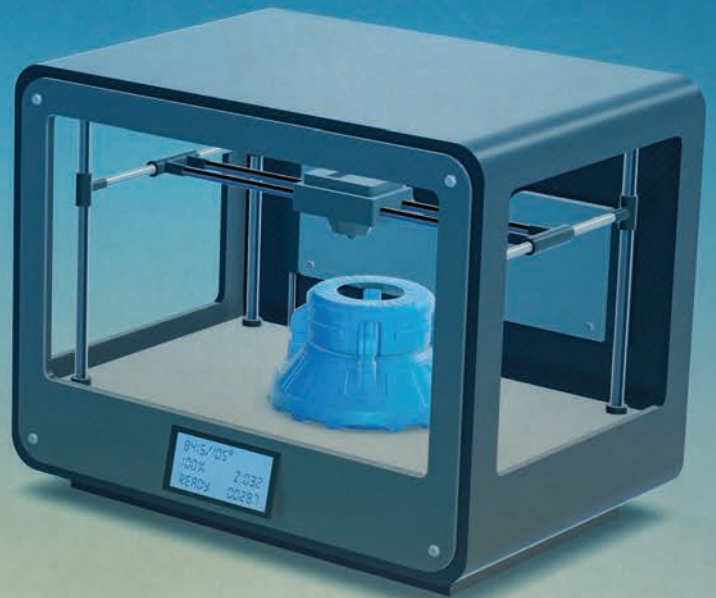
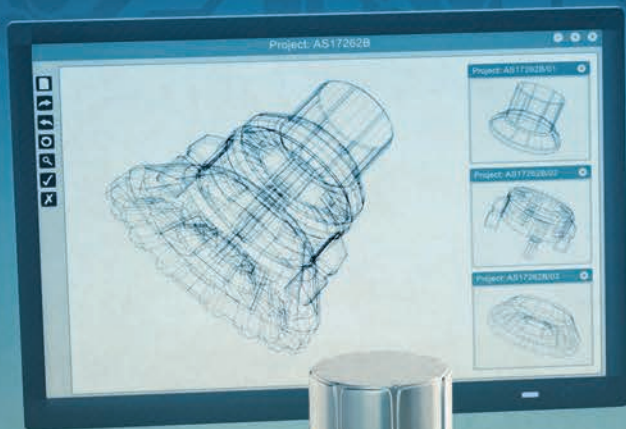
As militaries ready for the challenges presented by drones, they must also ensure that their own use of such technology is guided by transparent policies and rules that are subject to continuous review and revision in a swiftly changing environment. “Weapon systems with autonomous functionalities have been used safely and reliably in combat for eight decades. They will continue to be used in the future,” Robert O. Work, a former U.S. deputy defense secretary and retired U.S. Marine Corps colonel, wrote in his report titled “Principles for the Combat Employment of Weapon Systems with Autonomous Functionalities,” published in April 2021 by the Center for a New American Security. “Indeed, the addition of AI-enabled applications into these weapon systems is expected to make them even more discriminate in the application of force and lead to a reduction in unintended engagements — an aim entirely consistent with international humanitarian law.”

Nevertheless, unmanned weapon systems are not immune from human fallibility and error, and lessons must be gleaned from mistakes. For example, after a U.S. drone strike in Afghanistan in August 2021 killed 10 civilians, military leaders ordered an investigation of the tragic accident. The review by the U.S. Air Force inspector general found that the UAV operators believed they were targeting terrorists who planned to attack the Kabul airport, where a suicide bomber had killed scores of civilians and 13 U.S. service members days earlier.

Although the investigation found no violation of law, including the law of war, it concluded that “there were execution errors, combined with confirmation bias and communication breakdowns,” according to the U.S. Defense Department. Among other measures, the inspector general recommended implementing procedures to mitigate risks of confirmation bias, enhancing the sharing of mission situational awareness and reviewing prestrike procedures used to assess the presence of civilians.

Meanwhile, as the U.S. military continues to hone its counter-drone capabilities in conjunction with public and private collaborators, the demonstrations at the Yuma Proving Ground are expected to continue for several years. “Finally, we will work with our allies and partners to develop a shared understanding of threats, vulnerabilities, and interoperability needs,” noted the U.S. Defense Department’s Counter-Small Unmanned Aircraft Systems Strategy. “Through this holistic approach, the Department will ensure the Joint Force is both ready to meet today’s challenges and prepared for the future.” □

PRESS PRINT



Militaries Invest In 3D Printing
To Improve Force Efficiency
And Readiness

FORUM STAFF



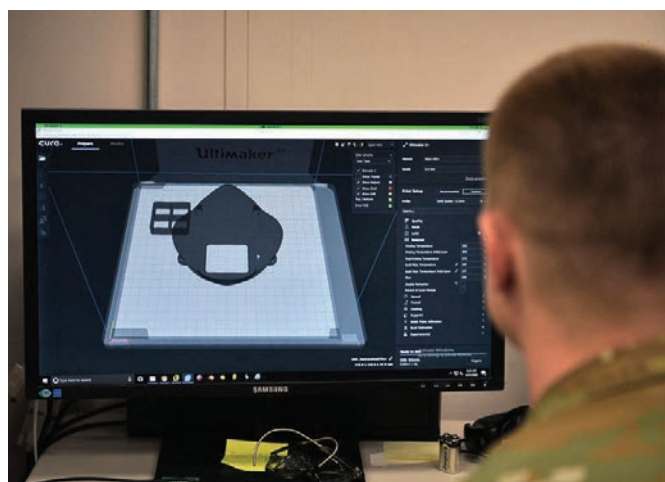
Rapid, on-demand and customizable technology such as 3D printing can help military personnel operate more efficiently whether on the battlefield or during a humanitarian relief mission. Militaries of the Indo-Pacific and elsewhere have invested heavily in research, development and acquisition of this force modernization tool.

Militaries have used the technology for at least the past decade to repair and replace weapons and parts for combat vehicles. United States forces in Japan used 3D printing to make face shields and masks to protect against COVID-19. The technology exists to 3D print bridges and houses. Now, there's even a plan to develop a 3D metal printer large enough to create a military truck exterior in one giant piece.

In the professional space, 3D printing is known as additive manufacturing (AM) — a process of joining materials to make parts from 3D model data, usually layer by layer. In the Indo-Pacific alone, spending on 3D printing is projected to swell to more than U.S. \$3.6 billion by 2024, according to AMFG, an autonomous manufacturing company headquartered in the United Kingdom.

“Globally, we’re already seeing policymakers rethinking how to weave in AI [artificial intelligence], automation and additive into their industrial strategies and policy,” Czek Haan Tan, general manager for the General Electric Additive Asia Pacific division, wrote for a GE.com blog in April 2021. “However, here in Asia — even before the pandemic — policymakers were already committing to advanced technology.”

China holds the largest share of the Indo-Pacific’s 3D printing market, followed by Japan, South Korea and the Association of Southeast Asian Nations bloc, respectively, according to a November 2019 AMFG report. Australia and India followed with a tied share of the market. U.S. spending on 3D printing outpaced the combined expenditure of the rest of the Indo-Pacific, and the European Union’s figures came in slightly less than those of the Indo-Pacific, AMFG reported. Other industry figures put Europe ahead of the Indo-Pacific.



A U.S. Air Force Airman prepares a 3D-printed N95 face mask to be printed through modeling software.

AIRMAN 1ST CLASS ROBYN HUNSINGER/U.S. AIR FORCE

“3D printing will revolutionize war and foreign policy ... not only by making possible incredible new designs, but by turning the defense industry — and possibly the entire global economy — on its head,” according to Business Insider. “The billion-dollar defense industry is at the ... edge of this innovation, with the U.S. military already investing heavily in efforts to print uniforms, synthetic skin to treat battle wounds and even food.”

As an industry leader, the U.S. regularly updates its 3D printing policy, including publishing a U.S. Department of Defense (DOD) Additive Manufacturing Strategy in January 2021. The document described AM as “a powerful tool to enable innovation and modernization of defense systems, support readiness and enhance warfighting readiness.”

3D printing can enhance military operations in three key ways, according to DOD. Among them:

- **Modernizing national defense systems.** “AM fundamentally changes how a component is designed by integrating the material, machine and design process to enable part geometries that

“ 3D printing will revolutionize war and foreign policy ... not only by making possible incredible new designs, but by turning the defense industry – and possibly the entire global economy – on its head.”

~ Business Insider

cannot be made using traditional manufacturing. These innovative designs can achieve greater operational performance. The performance of systems can also be improved by integrating printed material into or onto other components for sensors and electronic components.”

- **Increasing material readiness.** “AM can reduce the time-to-use, ensuring warfighters receive critical capabilities when needed. It enables the rapid production of prototypes, leading to decreased development times and faster iterations. An AM system is functionally a factory in a box,

a digitally controlled production line that can be turned on or off easily.”

- **Enhancing warfighting innovation and capability.** “AM allows tactical units to develop innovative solutions in theater. AM helps us shift the balance toward our greatest strength, the warfighter. Despite AM providing warfighters with increased capabilities, it must be balanced with safety guidelines, training and systems to support appropriate use.”

Bottom line: 3D printing enables the operation of more lethal systems, increased readiness and empowered warfighters who can solve problems in theater, in real time.

While 3D printing technology is advancing, militaries have been adapting its application for some time. For example, U.S. Soldiers in Afghanistan used a mobile 3D printing lab in 2013 to generate spare parts to repair equipment in the field rather than wait for a delivery, according to Dezeen magazine.

“The armed forces — from the U.S. to Australia — have recognized additive manufacturing’s potential for decades and have already put 3D printers to use in the field. 3D printed parts are currently in critical aircraft engines, on tanks and submarines and on the Soldiers themselves,” according to All3DP, a 3D printing magazine.



The world's first 3D-printed engine is displayed at the Australian International Airshow in Melbourne in February 2015. AFP/GETTY IMAGES



Soldiers can use 3D printers to make tools such as this wrench for field repairs. AFP/GETTY IMAGES



A U.S. Sailor holds a 3D-printed fuse box cover approved for shipboard use. SOUTHWEST REGIONAL MAINTENANCE CENTER

The Australian Army has extended through 2022 a collaboration with SPEE3D, a metal 3D printing company helping the Army's 1st Combat Service Support Battalion (1 CSSB) improve its supply chain through 3D printing of metal parts in the field.

"Custom made parts, designed and printed in the field, means we can get our equipment back in action and return to our primary role on the battlefield. We can strengthen the supply chain by employing modern technology like this to make exactly what we need at short notice," said Lt. Col. Kane Wright, commanding officer of 1 CSSB, according to an Australian Department of Defence story. "Our tech-savvy Soldiers now have the skills and the technology from SPEE3D to lessen the administration and logistics burden, to be their own solution without reaching back to base or a traditional commercial manufacturer."

Australia's pilot program proved that Soldiers can control the entire workflow, from designing spare parts to printing them, all from the field.

China's People's Liberation Army (PLA) held a public drill in 2015 demonstrating its use of 3D printing. During the drill, PLA soldiers noticed damage to their vehicle while responding to an oil tanker fire, 3DPrint.com reported. Without the necessary part in inventory, the soldiers used a 3D printer to become fully operational again instead of waiting for a technician to respond and repair the vehicle.

"The traditional way of machining parts is no longer necessary. No more planning, grinding, routing or other complex processes are required," said Dong Kaiyi, a PLA soldier participating in the drill, according to 3DPrint.com. "With the 3D printer now ready for use, say goodbye to a lot of heavy maintenance machines, as field repair efficiency has improved."

Open-source confirmation of advances in Chinese military technology can prove challenging, according to experts. The China Academy of Space Technology announced in mid-2020 that it had conducted its first

3D printing experiment in space — producing a flat section of a honeycomb-shaped structure and an emblem of the space academy's parent company, China Aerospace Science and Technology Corp., according to the PLA website China Military.

As with any technology, 3D printing comes with its challenges. Rand Corp. explores them in a report titled, "Additive Manufacturing in 2040: Powerful Enabler, Disruptive Threat."

"Some of the security implications are not difficult to imagine. As it becomes easier and cheaper to print weapons, the threat of kinetic attacks (i.e., violence through lethal force) could grow significantly," the Rand report said. "Through the internet, foreign terrorists and other violent extremists will likely have ready access to printable designs of new and more dangerous weapons. AM will also make it easier for homegrown dissidents and 'lone wolves' to print weapons quickly in locations where they previously would not have had access to them (for example, schools, government buildings, airports)."

Along with training, there must be heightened awareness about security risks to individuals, societies and militaries, Rand warned. Policymakers will also need to balance regulating 3D printing technology, to include proprietary protections, without unintentionally stifling the ability of militaries and others to use the technology for good, according to Rand.

"Any new technology brings potential benefits and threats. While fraught with risks, policymakers must begin to address the hard security questions that AM will bring. Decisions made today have the power to shape the opportunities and threats that will be faced in the future," the Rand report concluded, adding that more research should be done to understand potential security implications. "Now is the time to begin considering the awe-inspiring potential and possible negative consequences of this powerful new technology." □



An Indian Army convoy travels on the Srinagar-Leh highway at Gagangeer in Indian-controlled Kashmir.

THE ASSOCIATED PRESS



UNRESTRAINED CHINA

Bearing Down on India With Aggressive Lawfare

SAROSH BANA

The People's Republic of China's (PRC's) new Land Border Law laces its military threat to India with a legislative ultimatum.

The PRC's first national law on "protection and exploitation" of its land boundaries decrees that its sovereignty and territorial integrity are "sacred and inviolable." The law passed in October 2021 during the 13th National People's Congress and became effective at the start of 2022. The law is another example of PRC lawfare, whereby the regime develops domestic laws to justify its aggressive foreign and military policies.

The law applies to China's 22,457 kilometers of land borders with 14 countries, including Afghanistan, Bhutan, Kazakhstan, Kyrgyzstan, Laos, Mongolia, Myanmar, Nepal, North Korea, Pakistan, Russia, Tajikistan and Vietnam, but it selectively affects India. This is because the PRC claims to have settled its frontiers with 12 of these states, and it is pursuing a resolution with the Buddhist Himalayan kingdom of Bhutan that shares a trijunction with India and China at the Doklam plateau.

The border law heightens the hostilities between the two nuclear-armed powers, with a menacing PRC steering the situation perilously toward a flashpoint as it bears down on India

along their 3,488-kilometer Himalayan frontier, called the Line of Actual Control (LAC).

India has expressed concern over the law, which empowers the Chinese Communist Party's (CCP's) People's Liberation Army (PLA) to resort to armed reprisals against any perceived border transgressions and authorizes local administrations to increase border development projects. Responding to India's concerns, Chinese Foreign Ministry spokesman Wang Wenbin said Beijing "hopes relevant countries will abide by norms of international relations and refrain from wanton speculations on China's normal domestic legislation."

Beijing disputes most demarcations with India, despite three border agreements in 1993, 1996 and 2013. In 2017, the PRC had a 73-day standoff with India at Doklam that was the most critical in decades until the PLA incursion and occupation in May 2020 of swaths of land in the eastern part of India's Union Territory of Ladakh at the northwestern LAC. Also, the only full-fledged war between the two countries lasted a month in 1962, in which the PLA seized the 37,244-square-kilometer, high-altitude desert called Aksai Chin, which India claims as part of Ladakh. Following the 2017 skirmish in Doklam, the

PLA constructed military infrastructure and permanently deployed troops there.

Days before enacting its Land Border Law, the PRC agreed to a “three-step roadmap” with Bhutan to expedite negotiations to resolve the festering dispute over their 477-kilometer boundary. The PRC claims parts of Bhutan and has never officially recognized, nor even demarcated, Bhutan’s border with Tibet, which China annexed in 1951.

In November 2020, the PRC built a village 2 kilometers inside Bhutan and just 9 kilometers from the site of the India-China standoff in Doklam. The confrontation was triggered by the PRC’s attempt to extend a road in an area claimed by Bhutan, which has had a Treaty of Perpetual Peace and Friendship with India since 1949, a pact renewed in 2007. About 60,000 Indian nationals live in Bhutan, with an additional 8,000 to 10,000 visiting the country of about 780,000 daily from border towns to work.

India fears that the PRC’s intrusions are an indicator of what it views as “salami slicing,” whereby Beijing seeks to scythe through Indian and Bhutanese territory with the intent of redrawing the LAC.

SHADES OF THE SOUTH CHINA SEA

The Land Border Law uses a similar strategy to control territory as the PRC implemented under its so-called nine-dash line that demarcates its maritime claims in the South China Sea. The Philippines challenged the PRC’s claims in the region under the United Nations Convention on the Law of the Sea (UNCLOS). A tribunal at the Permanent Court of Arbitration at The Hague, Netherlands, ruled in 2016 that the PRC’s demarcation was without legal foundation and infringed on Manila’s sovereign rights. Several other similarly affected Southeast Asian nations that were not parties to the arbitration were heartened by the UNCLOS ruling.



Chinese troops dismantle their bunkers at the Pangong Tso region in Ladakh along the India-China border.

THE ASSOCIATED PRESS

Although the arbitration was considered final and legally binding, the PRC spurned the ruling.

The United States and numerous states worldwide have rejected the PRC’s claims in favor of the rules-based international maritime order within the South China Sea and worldwide, as stated in a January 2022 U.S. State Department study titled “Limits in the Seas No. 150.” The report concluded that “the overall effect of these maritime claims is that the PRC unlawfully claims sovereignty or some form of exclusive jurisdiction over most of the South China Sea. These claims gravely undermine the rule of law in the oceans and numerous universally recognized provisions of international law reflected in the Convention.”

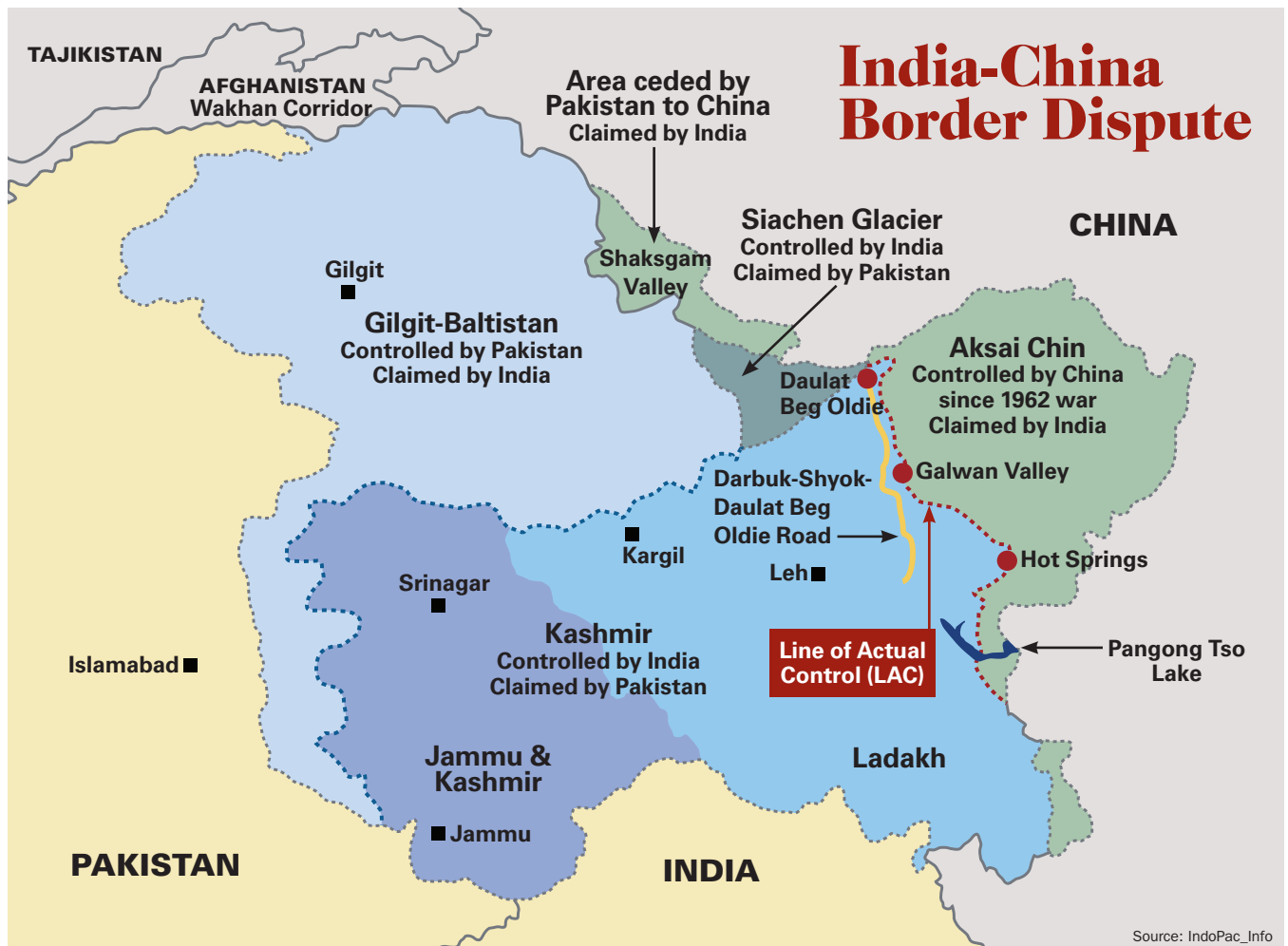
As part of its deception warfare at the LAC, the PRC has been constructing “dual-use” border villages and installations, where civilian settlements are being upgraded to military enclaves and civilian airfields converted into PLA Air Force bases. Satellite imagery has shown these developments, as well as PLA troop mobilizations along the LAC. The PRC is opening additional fronts along the border with India’s states of Uttarakhand, Arunachal Pradesh and Sikkim.

India also finds itself in a challenging situation, with 50,000 PLA troops still occupying parts of eastern Ladakh since their violent encounter with Indian Soldiers in the Pangong Tso area in May 2020. The brazenness with which the PLA troops have entrenched themselves at the spurs of Chang Chenmo on the northern lakeshore of the 135-kilometer-long Pangong Tso and staked claim to the whole of Galwan Valley contiguous to Aksai Chin exposes a tactical maneuver that has been devised with the intention of the troops remaining in the area.

Beijing chose summer 2020 for its border incursion as India was grappling with the economic and political challenges of the COVID-19 pandemic. The PRC may also have discerned a military vulnerability.

Tensions reescalated between the neighbors when their 13th round of corps commander-level talks collapsed in October 2021, failing to resolve the pending issues in eastern Ladakh. A statement by the PLA’s Western Theatre Command accused India of making “unreasonable and unrealistic” demands at the talks, which lasted less than nine hours. The Indian Army countered, “During the talks, the Indian side made positive suggestions to resolve the issues in other areas, but the Chinese side did not seem to agree with them and could not even make any proposal on the way forward.” It added that Beijing had made “unilateral attempts” to alter the status quo at the LAC and was thus obliged to take appropriate steps to restore peace in the region.

A day before the talks, Indian Army Chief Gen. M.M. Naravane expressed concern at the PLA’s continuing large-scale buildup in eastern Ladakh. “It means that they are there to stay,” he said. “We are keeping a close watch on all these developments, but if



they are there to stay, we are there to stay, too.”

The standoff still simmered as of late 2021, with troops ranged against each other in the desolate but strategic Himalayan desert.

CONTINUING TENSIONS

Even as the PLA continued to occupy two friction points — Patrolling Point (PP) 15 in Hot Springs and PP17A near Gogra Post in Ladakh along the LAC — China has amassed additional troops across the border, armed with artillery, air defenses, combat drones and heavy vehicles. Some of them reportedly crossed the LAC in July 2021 to reoccupy positions on the Kailash Range they had vacated following a February 2021 demilitarization agreement, and others moved to points near the Galwan river and Pangong Tso.

In all of the military-level talks and diplomatic engagements on the issue, India has taken the stand that de-escalation is possible only if complete disengagement takes place. The PRC has held its ground, accusing India of causing the border flare-ups by violating the LAC.

The PRC seems intent on drawing India out by upping the ante at various friction points along the LAC. India appears to be left with little option but to tread with

caution, lest this feuding escalate into a war it can ill afford.

Beijing has, moreover, been emboldened by India’s response after the PLA killed 20 Indian Soldiers in eastern Ladakh on June 15, 2020, in the first deadly skirmish since the 1962 Sino-Indian war. The India government retaliated later in 2020 through a ban on 267 apps originating from China, prompting a trending refrain on India’s social media: “They changed our map, we banned their app.”

Though it is vigorously creating military infrastructure at the LAC, the PRC resents any required activity by India, such as its recently inaugurated 50-meter bridge on the Leh-Loma Road that the Indian Defence Ministry says will ensure “unhindered movement of heavy weapon systems, including guns, tanks and other specialized equipment.”

The PRC’s adventurism may have its genesis in its contempt for India’s completion in 2019 of the 255-kilometer Darbuk-Shyok-Daulat Beg Oldie Road, which runs at elevations between 4,000 and 5,000 meters and has improved connectivity along the 1,147 kilometers of the LAC in eastern Ladakh. The carriageway leads to the world’s highest airstrip and military base (of India) at Daulat Beg Oldie, which lies 12 kilometers south of

An Indian fighter jet flies over a mountain range in Leh in the Ladakh region.

REUTERS



the strategic 5,540-meter-high Karakoram Pass north of Aksai Chin on the boundary between Ladakh and China's Xinjiang Uyghur Autonomous Region. Just 7 kilometers north is Shenxianwan, considered to be the toughest PLA posting in China.

The Indian Ministry of Defence's Border Roads Organisation is reportedly building 70 roads of operational significance along the border with China, as well as widening and strengthening existing roads and building advance landing grounds, tunnels and bridges.

China, in turn, has built a 36-kilometer road in the 5,163-square-kilometer Shaksgam Valley, which was illegally ceded to it by Pakistan in 1963, while the territory was disputed by India.

LADAKH LINES

China was outraged enough by India's abrogation in 2019 of its Articles 370 and 35A, which resulted in the reorganization of the frontier state of Jammu and Kashmir, of which Ladakh was then a part, to take the matter to the U.N. Security Council. It was particularly incensed over the change in Ladakh's political status because China considers the region to be of strategic importance. India rebuffed China, terming Ladakh's new status an "internal matter" that had "no implication for India's external boundaries or the LAC with China." The Chinese Foreign Ministry, however, issued a statement asserting, "The recent unilateral

revision of domestic laws by the Indian side continues to undermine China's territorial sovereignty, which is unacceptable and will not have any effect."

Beijing also took offense at Union Home Minister Amit Shah's assertion in the Indian Parliament that: "Kashmir is an integral part of India. I want to make it absolutely clear that every single time we say Jammu and Kashmir, it includes PoK [Pakistan-occupied Kashmir], including Gilgit-Baltistan, as well as Aksai Chin. Let there be no doubt over it. Entire Jammu and Kashmir is an integral part of the Union of India."

Gilgit-Baltistan connects to the China-Pakistan Economic Corridor (CPEC) being funded with U.S. \$60 billion in Chinese investment and is the flagship of China's One Belt, One Road scheme. From Beijing's perspective, any Indian attempt to take over PoK or Gilgit-Baltistan would undermine the CPEC, in which Xi has staked his personal prestige because it provides China access to the Indian Ocean through Pakistan's Gwadar port. India contends that the CPEC violates its territorial sovereignty by passing through Gilgit-Baltistan.

In mid-October 2021, Shah also sounded a stern warning to India's adversaries against "flirting" with the nation's borders, affirming that every such act would be met with "befitting retaliatory moves by India."

Beijing has been evidently provoked by such utterances. Overall, its military offensive against India



is not merely tactical but has a strategic intent aimed at realizing long-term objectives. The PLA's moves are, after all, being directed by its top leadership, the CCP's Central Military Commission chaired by Xi.

EMERGING DIPLOMACY

Veteran U.S. diplomat Nicholas Burns noted in October 2021 that the alignment of U.S. and Indian interests in the Indo-Pacific “makes a great difference” in terms of the challenges posed by the PRC. “As you know, and I think every administration since President [Bill] Clinton has been working on this, we have a newfound security partner in India,” Burns said during his confirmation hearings as U.S. President Joe Biden’s nominee to be the nation’s ambassador to China. “That makes a great difference to have Indian and American interests aligned as they clearly are, strategically, in the Indo-Pacific.”

While the U.S.-India military relationship continues to reach new heights, the mistrust between China and India is mounting, Adm. John C. Aquilino, now U.S. Indo-Pacific Command commander, said during his confirmation hearing in March 2021 before the Senate Armed Services Committee. He commended India’s efforts to protect its northern border during its standoff with China in his testimony, CNBC reported.

“The mistrust between China and India is at an

all-time high. In addition to the rupture of bilateral relations as a result of the LAC (Line of Actual Control) skirmish, India is deeply suspicious of Chinese activities as part of the ‘One Belt, One Road’ initiative,” Aquilino said.

“China’s posture initiatives in both Gwadar, Pakistan, and Hambantota, Sri Lanka, also cause India concern. As is the case across the Indo-Pacific, [the] PRC’s lack of transparency and duplicitous actions in the Indian Ocean region threaten stability and security in the region,” he wrote in a prepared response to questions from Senators for the confirmation hearing.

Recent activities by the PRC have underscored the threat it poses to all nations and the need for greater cooperation between India and the U.S., he said. “The conclusion of enabling agreements over the past several years has allowed us to operate more closely, and we are able to work together more than ever before to secure a Free and Open Indo-Pacific,” he said, citing the continuing growth of bilateral and multilateral engagements, high-profile joint operations and an increased number of senior-level engagements with India, according to CNBC.

The military threat from the PRC has become a defining moment for India. How the nation emerges from it will ultimately determine its standing in the global community and its stature in the international alliance on security. □



FORUM ILLUSTRATION

FIGHTING *for* DIGITAL FREEDOM

Competition for dominance over information technology ecosystems underpins the battle between democratic and authoritarian rule

— FORUM STAFF —

Thousands of Cubans flooded the streets in July 2021 to protest their government's failure to provide food, medicine and other necessities amid the COVID-19 pandemic. Within days the communist regime shut down the country's internet and telephone communications, blocking the broadcast of widespread discontent to the outside world for several days. Cuba not only borrowed a page from the Chinese Communist Party's playbook on how it controls its citizens, but Chinese technologies and companies, which built Cuba's telecommunications infrastructure, made this type of censorship possible.

Repressive regimes such as Cuba are increasingly looking to the People's Republic of China (PRC) to provide digital tools for domestic surveillance, monitoring and censorship to manipulate domestic and foreign populations and to promote their authoritarian form of rule, according to a series of reports by leading security think tanks.

Elements of the Chinese government's brand of high-tech repression, used most prominently to control minority populations in Xinjiang province, have been installed in other parts of China and exported to dozens of countries in Africa, Latin America, Eastern Europe and Southeast Asia, as the reports detailed. At least 50 countries are developing surveillance systems supported by technologies supplied by Chinese firm Huawei, a 2019 report by the Carnegie Endowment for



Riot police walk the streets July 12, 2021, after a large, anti-government demonstration in Havana, Cuba. AFP/GETTY IMAGES

International Peace revealed. Russia's relatively lower-tech disinformation tools have also been exported to dozens of countries to help repress opposition at home and foment civil discord in democracies abroad, as Dr. Alina Polyakova and Chris Meserole chronicled in a 2019 Brookings Institution report, "Exporting Digital Authoritarianism: The Chinese and Russian Models."

More moderate governments, even some democracies such as Serbia and Uganda, have also been enticed by the promises of control these technologies offer despite the long-term repercussions of their use, as Erol Yayboke and Sam Brannen explained in a 2020 report for the Center for Strategic and International Studies (CSIS), titled “Promote and Build: A Strategic Approach to Digital Authoritarianism.”

The trends have only accelerated since the reports came out. “Authoritarian-led states have continued to use digital means to repress their citizens, often using the COVID-19 pandemic as an excuse to enact even more strict controls,” Yayboke, who is now director of CSIS’s Project on Fragility and Mobility, told FORUM. “For example, location and virus testing data can be collected for public health reasons but can also be used as a way for governments to keep closer tabs on their citizens. But what most concerns me is the emergence of these trends in ostensibly nonauthoritarian-led countries. One tool in particular — data localization — is being used more often under the guise of ‘privacy’ and ‘national security.’”

Although the motivations for using these technologies may vary greatly, “in many cases, democratic or partially democratic countries are turning to such technologies (many of which originate in places like China and Russia)

because they are cheapest and sometimes the only available ones to them. Others may feel that, especially during a pandemic, knowing more about citizens is more beneficial than knowing less, perhaps even convincing themselves that these increased control measures are temporary, put in place in an emergency,” Yayboke said. “History tells us though that this type of increased control, even if originally meant to be short-term and for nonmanipulative reasons, is tough for leaders to relinquish.”

Allies, partners and like-minded nations must work together to put forth a competitive democratic model of digital governance to counter the spread of digital authoritarianism, experts agree. The systems must increase security but protect civil liberties and human rights and be introduced with established norms of conduct, asserted Meserole, who is research director for Brookings Artificial Intelligence and Emerging Technology Initiative, and Polyakova, now president and CEO of the Center for European Policy Analysis.

Militaries can play a critical role in establishing and protecting digital democracies, other experts contend, despite that some nations are deploying their militaries to perpetuate digital authoritarianism. Increasing public awareness about the manipulation and control of information is also a key part of the solution, experts agree.



A car passes the National Capitol Building in Havana, Cuba, on July 12, 2021, a day after thousands of demonstrators took to the streets, chanting “down with dictatorship.”

AFP/GETTY IMAGES

“Democracies must recognize that we are in a geopolitical battle over the digital governance model that will dominate in the 21st century,” concluded a June 2021 report by the Task Force on U.S. Strategy to Support Democracy and Counter Authoritarianism, which was established by Freedom House, a nonprofit nongovernmental organization, CSIS and the McCain Institute for International Leadership at Arizona State University in September 2020.

TAIWAN’S MODEL

Taiwan, for example, is developing a leading model for digital democracy based on its goals for parliamentary reforms. Its model strives to use emerging technologies to facilitate transparency, openness, participation, digitization and literacy, the online magazine *The Diplomat* reported in July 2021.

Digital democracy is founded on civic-tech, the use of technology to create democracy and give citizens a vote, Min Hsuan Wu, also known as Ttcat, explained to *The Diplomat*. He co-founded Doublethink Labs, an organization created in 2019 to research threats to democracy and devise ways to counter them. Meanwhile, digital authoritarianism relies on tools ranging from those for repression and disruption, such as surveillance, espionage, cyberattacks, censorship, and social and electoral manipulation, to those for strategic competition, such as technologies that enable digital infrastructure, control of internet service systems and data localization, Yayboke said.

“While Beijing uses digital tools such as the social credit system and state censorship, in Taiwan the social sector actively creates digital infrastructures to enable everyday citizens to propose and express opinions on policy reforms,” Taiwan Digital Minister Audrey Tang told *The Diplomat*. “In a digital democracy, transparency is about making the state transparent to the public. Under digital authoritarianism, the word ‘transparency’ means making citizens transparent to the state.”

Lessons learned and technologies developed to reform Taiwan’s government are readily transferrable to other democracies. Although none of the emerging models is perfect, Yayboke said Denmark and Estonia also have built good models of digital democracies that might be shared with other nations.

“For China, maybe only one thing is certain, that the propaganda narrative they ran for years — that democracy is not for Asia — is no longer appealing under Taiwan’s progress,” Ttcat told *The Diplomat*.

DEFENDING DEMOCRACY

Along with competitive models, approaches that restrict the supply of technologies that enable digital authoritarianism, such as sanctions and export controls, could help curb deployment of such systems, several of the think tank reports suggested. However, the problem is complex in part because of the maturity of the surveillance economy. Although China is the largest supplier of surveillance

systems, nations including France, Israel, Russia, the United Kingdom and the United States also supply advanced technologies that can be used to facilitate population-scale control, as Meserole and Polyakova noted.

The U.S. and many European countries have taken steps to limit the export of advanced processors and sensors that enable mass surveillance systems, which continue to mainly be manufactured in Western countries, as the Brookings report stated. For example, the administration of then-U.S. President Donald Trump blocked global chip supplies to Huawei in May 2020 to impede the company’s expansion, Reuters reported. Such measures may be slowing the proliferation of mass surveillance systems, given that the PRC has made little progress in achieving self-sufficiency in semiconductors and its large subsidies for semiconductor projects have failed to produce successes, according to news reports. China’s self-sufficiency ratio for semiconductors is expected to be only 19.4% in 2025, a May 2021 article on the *Nikkei Asia* website reported.

The COVID-19 pandemic accelerated the timetable for Europe, North America and other regions to reduce supply-chain dependence on China by not only highlighting the issue but also raising fears among Western and Indo-Pacific businesses about the data security and privacy risk related to collaborating with Chinese companies on technology endeavors. For example, India banned 59 Chinese apps from its domestic market in January 2021, news agencies reported. Yet, long before the pandemic, many countries, including Australia, had already blocked Huawei from supplying their 5G networks.

The U.S. has launched multiple initiatives to counter digital authoritarianism by increasing competitiveness through efforts that move beyond imposing economic restrictions to decouple the U.S. and Chinese economies. The U.S. Defense Advanced Research Projects Agency (DARPA) is funding artificial intelligence (AI) research to better understand digital authoritarianism with projects that range from detecting misinformation and deep fakes online to analyzing information operation campaigns. Legislators are pushing several initiatives to revamp microelectronics production and bolster U.S. technology competitiveness. In March 2020, legislation was introduced in the U.S. Senate to create an international partnership, led by a new U.S. State Department office, to counter the influence of authoritarian governments such as China on emerging technologies. The office would forge a path to set international technology standards, among other goals.

Collaboration is key for countering digital authoritarianism, according to Mieke Eoyang, U.S. deputy assistant defense secretary for cyber policy. “We need to make sure that we are offering alternatives to allies when they are thinking, when they are considering their own technology purchases, and we need to do a better job of sharing the risks and vulnerabilities that our allies and partners might incur if they were to engage in purchasing such technologies,” Eoyang told Nextgov.com.

“Often, these data localization mandates are put forth under the guise of ‘protecting’ individuals’ privacy or security, but the result is often the exact opposite.”

— Erol Yayboke, director of the Center for Strategic and International Studies' Project on Fragility and Mobility

The Information Technology and Innovation Foundation (ITIF), an independent policy think tank based in Washington, D.C., issued a report in mid-June 2021 pushing for the U.S. to establish an independent agency to drive a national technology strategy to compete with China as well. The proposed National Advanced Industry and Technology Agency would have a budget comparable to the National Science Foundation, which is more than U.S. \$8 billion annually, and have five divisions: data and analysis, advanced industries, emerging technologies, innovation systems and cross-agency and cross-government coordination.

“There are many steps Congress and the administration should take to compete against China, but the best way to completely change the game would be to create a specialized agency with a focused mission and sufficient resources to bolster the competitive position of advanced technology industries,” Robert Atkinson, ITIF president and author of the report, said in a June 2021 statement.

Still others contend that shoring up democracy is critical for countering digital authoritarianism. Leading democracies, such as the U.S., need to strengthen trust in domestic institutions by expelling foreign intervention in elections, supporting free and fair elections, committing to peaceful transitions of power and limiting misinformation and spread of conspiracy theories, Yayboke and Brannen argue in their CSIS report.

The June 2021 report from the Freedom House-led task force goes further. It recommends: “The United States should embrace a ‘diplomacy of democracy,’ making democracy and countering authoritarianism a priority for U.S. diplomatic engagement. That prioritization should include galvanizing an international coalition to push back against authoritarian threats and reinforce democratic governance. Our fundamental approach should be one of partnership and solidarity with governments, civil society organizations, universities, the private sector and citizens working to confront these challenges together.” U.S. President Joe Biden’s Summit for Democracy, held December 2021, presented an ideal opportunity to do just that, the task force noted.

Allied nations and partners must also promote democratic and human rights principles abroad and promote free online expression and secure communication, Meserole and Polyakova recommended. “To build resilience against foreign influence operations in democratic societies, governments should invest in raising public awareness around information

manipulation,” they wrote. “This should include funding of educational programs that build digital critical thinking skills among youth.”

MILITARY ROLE

Defense leaders and security professionals, however, should not wait for the rest of the government to act, Joshua Baron, a DARPA program manager, told FORUM. “The notion of digital authoritarianism is not just an issue within foreign policy circles but within national security circles,” he said.

Technologies that enable digital authoritarianism make operating in such environments more challenging for allies and partner militaries. For example, tools that facilitate real-time surveillance and internet blocking can weaken operational security, Baron said. “To the degree that the [U.S.] Defense Department operates over the internet, everything we do has a digital footprint. As countries have better capabilities to control that environment, it will have implications for us.”

Countries that are heavily invested in population-scale surveillance technologies, for example, could have an advantage in using them to influence U.S. allies and partners given the defense community has not historically considered them to be weapons, Baron said. Other tools related to digital authoritarianism could be used to “enable domestic influence and control operations that can shore up public support for a revisionist regime and embolden it to conduct similar operations against American audiences,” Baron explained in a June 2021 article for DefenseOne.com.

DARPA has funded several programs to create tools to counter such capabilities by helping the military and citizens understand the truth about what’s really happening on the ground, Baron told FORUM. For example, it’s developing an attack-resistant mobile communication network for use in a contested environment. Known as Resilient Anonymous Communication for Everyone (RACE), the project will enable users to evade large-scale adversary targeting using encryption and protocol embedding strategies, said Baron, who oversees the program. RACE technologies may also mitigate denial of service attacks and protect privacy.

DARPA has also launched a program, called Measuring the Information Control Environment (MICE), to develop AI technology to measure how authoritarian regimes repress their populations at scale over the internet via censorship, blocking and throttling, Baron

said. “MICE-developed technology will continuously and automatically update and feed into easily-understood dashboards in order to develop comprehensive, real-time ground truth understanding of how countries conduct domestic information control,” according to DARPA.

The security risks for nations and militaries from surveillance, censorship and hacking capabilities continue to grow. For example, some governments are employing data localization policies to limit democracy and human rights as an extension of digital authoritarianism. “Tighter controls on the cross-border flow of data are an emerging concern,” Yayboke told FORUM. By territorializing data, governments can better execute crackdowns on free expression, privacy and human rights, Yayboke explained in a July 2021 CSIS policy brief.

“Often, these data localization mandates are put forth under the guise of ‘protecting’ individuals’ privacy or security, but the result is often the exact opposite. When citizen data — from Google Maps searches to Instagram likes to TikTok posts — is forced to be stored on local servers, governments have greater opportunities to use these data to gain greater control over the population. From Bangladesh to China to Russia and beyond, this manipulation enhances and strengthens the modern digital surveillance and censorship state,” Yayboke wrote in the brief, titled “The Real National Security Concerns over Data Localization.”

Data localization can also restrict collaboration among military, law enforcement, intelligence and other security professionals by blocking access across borders. “It effectively provides a safe haven for actors who execute gray zone tactics, including information operations via social media and illicit financial activities, on platforms subject to localization requirements — limiting the ability of targeted countries to combat and investigate them and, if applicable, prosecute the perpetrators of related crimes,” Yayboke wrote.

“If U.S. friends and allies adopt stricter data localization requirements, it could further complicate an already convoluted and outdated mutual legal assistance treaty system, increasing barriers to law enforcement in the growing number of cases involving data that flowed across international borders. This would weaken current information-sharing channels and businesses’ reporting obligations, thereby impacting intelligence-gathering methods and criminal investigations.”

DIGITAL STRATEGY REQUIRED

The proliferation of such activities makes the need for a cohesive digital strategy more urgent — one that forms the foundation for a principles-based approach among like-minded nations, experts agree. “In short, the tools of digital authoritarianism are effective for control and manipulation. Malign actors foreign and domestic can use them in ways that are fundamentally misaligned with democratic principles, for example, via disinformation campaigns that use slickly presented falsehoods to gain electoral advantage,”



Residents watch security personnel in Kashgar in western China's Xinjiang region. Authorities are using detention centers and data-driven surveillance to impose a police state on Uyghurs and other Muslim minorities in the region. THE ASSOCIATED PRESS

Yayboke told FORUM. “But the fundamental goal of many such actors is actually not direct manipulation but rather in sowing mistrust in the institutions of democracy: elections, civil society groups, independent expertise, etc. In this regard, the tools of digital authoritarianism are unparalleled in their effectiveness.”

For all these reasons, the U.S. and its allies and partners must offer better choices for digital governing and surveillance than Chinese technologies and Russian tactics offer, experts agree. Allies and partners need to develop tools to provide privacy, guarantee internet freedom and counter influence campaigns. Like-minded nations must work with tech companies and nongovernmental organizations to develop a code of conduct for managing personal data, establishing common standards across platforms and addressing social media manipulation, as Meserole and Polyakova recommended.

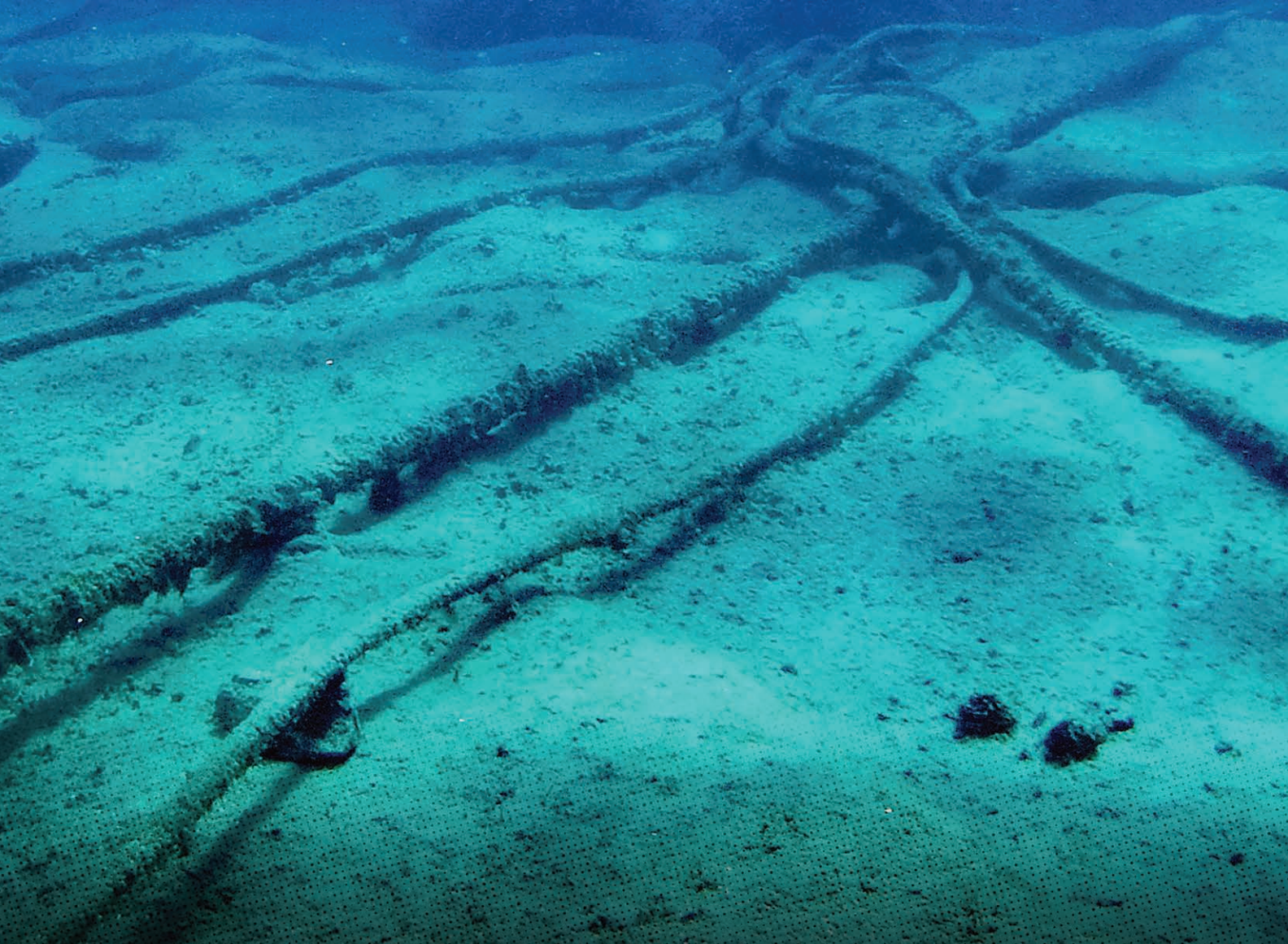
Nations must work together to develop research strategies and whole-of-government approaches to counter digital authoritarianism, including building multilateral coalitions, as Yayboke and Brannen advocated. For example, nations should collaborate with industry to ensure continued participation and representation of democratic interests on international technology standards-setting bodies, such as the United Nation's International Telecommunication Union and the World Trade Organization, they suggested.

Defense professionals can lead the way by developing tools to help understand the digital playing field and shore up their militaries' advantages on the digital battlefield, DARPA's Baron added. “Security forces the world over are getting more digitally sophisticated. They can collect and assess data more effectively and efficiently and then bring real-world enforcement capabilities to these perceived threats that originate online,” Yayboke agreed. □

UNDERSEA CABLE WARS

FORUM STAFF

COMPETITION FOR CONTROL OF NETWORKS BRINGS
LONG-TERM SECURITY RISKS TO THE SURFACE



A labyrinth of more than 1.3 million kilometers of fiber-optic cables anchored to the sea floor carries about 95% of telephone and internet communications around the world every day, moving massive amounts of data every second. Everything from financial transactions to military orders passes along this underwater web of more than 475 cables.

The security implications of this critical infrastructure are clear: Whoever controls the lines possesses significant power. As data has become an increasingly important strategic asset, the security risks could be substantial under certain circumstances, experts said. Although shipping and fishing operations cause most of the damage to the cables and natural events such as earthquakes, cyclones and even shark bites can interfere with operations, the prospect of intentional, malicious damage looms large, as the amount of data traversing the transoceanic cables continues to grow and reliance on cloud storage increases.

“Regarding physical challenges, the two primary concerns are that the cables might be destroyed or tapped — by either a non-state actor, as per some recent isolated incidents of piracy, or, more likely,

by a state adversary like Russia,” according to Pierre Morcos, a visiting fellow with the Europe, Russia and Eurasia Program at the Center for Strategic and International Studies (CSIS) in Washington, D.C., and Colin Wall, a research associate with the same program. “There are several conceivable objectives severing a cable might achieve: cutting off military or government communications in the early stages of a conflict, eliminating internet access for a targeted population, sabotaging an economic competitor, or causing economic disruption for geopolitical purposes. Actors could also pursue several or all of these objectives simultaneously,” Morcos and Wall contend in a June 2021 article published on the CSIS website, titled “Invisible and Vital: Undersea Cables and Transatlantic Security.”

Governments, companies or organizations could also tamper with cables in more insidious ways such as exfiltrating data via backdoors inserted during the manufacturing process, stealing data from onshore facilities that connect to the undersea cables or perhaps even harvesting data at depth, Dr. Amanda Watson, a research fellow at the Australian National University, told FORUM. There is also a “general cybersecurity risk increase because you might have citizens, businesses or utilities that could be victims

Sri Lankan engineers and divers maintain an undersea cable, laid by an Indian-owned telecommunications company, in Colombo. AFP/GETTY IMAGES





An operator moors an undersea fiber-optic cable near Sopelana, Spain. The connection is part of the more than 6,600-kilometer Marea cable, funded by Facebook and Microsoft, now stretching between Spain and the United States. AFP/GETTY IMAGES

of cybercrime, cyberattacks, ransomware or theft of data,” said Watson, who has studied the telecommunications industry and mapped cable deployment in the Pacific islands region for more than a decade.

“The security and resilience of undersea cables and the data and services that move across them are an often understudied and underappreciated element of modern internet geopolitics,” according to a September 2021 report from the Atlantic Council, an international economic and political think tank. “The construction of new submarine cables is a key part of the constantly changing physical topology of the internet worldwide,” said the report, titled “Cyber Defense Across the Ocean Floor: The Geopolitics of Submarine Cable Security.”

Authoritarian governments, such as the People’s Republic of China (PRC), could exert control over state-run companies to route the global data to their advantage, for example, for espionage purposes, asserts report author Justin Sherman, a fellow at the council’s Cyber Statecraft Initiative. In addition to ongoing concerns about China’s largest undersea cable supplier, HMN Technologies, which until recently was called Huawei Marine, several Chinese-incorporated firms that are listed as owners of undersea cables, including China Mobile, China Telecom and China Unicom, are all state-owned, Sherman wrote. “Changes to traffic routing patterns generate profits for companies and can move new volumes of traffic through different countries’ borders. This can enable data interception and the development of technological dependence.”

Moreover, companies that manage undersea cables have introduced operational risk through network management systems to centralize control over

components, according to the report. “When these cable management tools are connected to the global internet, they expose undersea cables to new risks of hacking — both for monitoring cable traffic and disrupting it altogether,” Sherman wrote.

As the technology and its deployment evolve, the risks only continue to grow. For a start, the proliferation of cloud computing has increased the volume of data flowing over the internet. This, coupled with the growth trend in remote work due to the COVID-19 pandemic, has also significantly increased the sensitivity of the data. Meanwhile, security is often not a top consideration in the planning, production, installation and maintenance of the cables because growing segments of the world’s cable infrastructure are controlled by a mishmash of private sector and state-run companies with other priorities.

INCREASED STAKES

Given the stakes, the undersea cable industry has become one of the latest realms of power competition between the United States and China, especially in the Indo-Pacific region. To mitigate security risks, U.S. allies and partner nations must continue to offer better alternatives to Chinese-backed cable infrastructure, experts assert. Although tensions between the U.S. and China may have delayed some cables from being installed, security protections are worth the wait, they said.

The U.S. and many of its allies and partners have been concerned for many years over the expansion of various state-owned companies or firms with Chinese Communist Party ties into the undersea cable business as a component of the PRC's strategy to increase its global reach. "This is another vector by which Huawei gets into the infrastructure of another country," retired Lt. Gen. William Mayville, former deputy commander of U.S. Cyber Command, told *The Wall Street Journal* newspaper in 2019. "Failing to respond to Huawei Marine cedes space to China," he said. "The U.S. and its partners must meet and compete." In June 2020, the U.S. Commerce Department placed Huawei on its Entity List, which restricts the sale of U.S. goods and technology to the company, and within months added most of Huawei's subsidiaries, including Huawei Marine.

Huawei Marine, founded in 2008 as a Huawei subsidiary, built or repaired more than 90 of the world's undersea cables before being sold to Shanghai-based Hengtong Optic-Electric in 2019. "But the sale failed to alleviate national security concerns: Hengtong's director and founder is a Chinese government official," explained Nadia Schadow, a senior fellow at the Hudson Institute, in a July 2020 article in *Defense News*. In 2020, Huawei Marine rebranded itself as HMN Technologies but is still subject to U.S. Commerce Department restrictions, Reuters reported.

HMN Technologies, with a roughly 10% market share, has emerged as the fourth-largest undersea cable provider after Alcatel Submarine Networks, based in France; SubCom in the U.S.; and NEC in Japan. However, content providers, such as Amazon, Facebook, Google and Microsoft, are expanding their market presence, owning or leasing at least half of the global undersea bandwidth. Facebook and Google, for instance, revealed in 2021 that they plan to lay two underwater cables to connect the U.S. to Indonesia and Singapore, increasing the capacity for data transfer between North America and Southeast Asia by 70%, Reuters reported. Most Southeast Asian internet users access via mobile data, so new undersea cables will improve bandwidth. Only about 10% of Indonesia, for example, has access to broadband internet, according to a 2020 survey by the Indonesian Internet Service Providers Association.

Content providers' entry into the market, however, has complicated security risks, experts said. Partnerships or arrangements with the already powerful tech companies could grant governments access to information that flows through their cables. Conversely, content providers could restrict access to information to gain leverage over governments. As it is, laws governing undersea cables and their ownership are not fully developed.

PACIFIC ISLANDS PROGRESS

The Pacific islands region has been an epicenter of undersea cable competition in recent years, as governments and citizens have sought better internet

connections to advance their economic development. In 2007, only four Pacific islands nations and territories were connected by undersea cables, but almost all Pacific islands nations are poised to connect within the next several years, according to the U.N.'s International Telecommunication Union.

In this region, allies and partner nations have fended off several Chinese bids to install cables given the security risks. The Federated States of Micronesia announced in early September 2021 that it would rely on U.S. funding to build a cable between Kosrae and Pohnpei, rejecting a Chinese-led bid due to security concerns, Reuters reported. The World Bank declined to award the project in June 2021 after the U.S. objected to the contract being awarded to HMN Technologies. The original project would have also connected the Pacific islands nations of Nauru and Kiribati, according to Reuters.

In 2017, Australia blocked a plan by Huawei Marine to link Sydney with the Solomon Islands via a 4,000-kilometer cable. In the end, Australia funded construction of the cable known as the Coral Sea Cable System, which connects Port Moresby in Papua New Guinea and Honiara in the Solomon Islands to Sydney, CNN reported. "The concern was China could have an ability to in-build security vulnerabilities," an Australian security official told *The Wall Street Journal* in 2019. "It really mirrors the issues with 5G," he said.

"That was seen as a red line that Australia would not cross and so we jumped in with a better deal providing the cable as a grant that would be implemented with a procurement partner of Australia's choosing — that wouldn't be Chinese," Jonathan Pryke, director of the Lowy Institute's Pacific Islands Program, told Australia's ABC News in June 2021. Australia has also been discussing plans to connect Nauru to the Coral Sea Cable System, Reuters reported.

"One key difference between arrangements with China and with other countries is China's offers had to be through loans where Australia and similar countries tend to give gifts," Australia National University's Watson told FORUM. As more cables continue to be installed in the region, Watson would like to see a more holistic strategy emerge from partner nations, such as Australia, Japan, New Zealand and the U.S., to meet the needs of Pacific islands nations.

Australia is also working with Pacific island nations to improve the reliability of existing networks by increasing resiliency and redundancy. In January 2022, for example, a volcanic eruption damaged Tonga's main undersea cable, which connects to Fiji, highlighting the vulnerability of the technology. Hopefully, additional cables will be installed to avoid extensive outages in the future, security officials said.

Chinese firms, meanwhile, often submit bids at a lower cost, but the quality is also lower, according to Pryke. Nations in "the Pacific are wising up to China. They do recognize a lot of the quality of infrastructure they've

received has been lackluster from China, so they are putting more pressure on Chinese businesses to put in reasonable bids,” he told ABC News. Huawei Marine built a domestic undersea cable for Papua New Guinea that has had ongoing technical issues and is largely viewed as an investment failure, according to ABC News.

Analysts have watched similar scenarios play out in other parts of the developing world from South Asia to Africa under the PRC’s so-called digital silk road initiative that entails building undersea cables and terrestrial and satellite links as a component of China’s One Belt, One Road infrastructure scheme. Although host nations may benefit somewhat from the construction, most of the projects are being built, financed and controlled by the PRC, placing many countries at a high risk of debt distress, according to the International Monetary Fund. This can lead to loss of sovereignty and enable the PRC’s power projection globally.

Consider China’s installation of an Asia-Africa-Europe undersea cable, funded by the China Construction Bank, to connect with Hong Kong, Vietnam, Cambodia, Thailand, Malaysia and Singapore, then onward to Myanmar, India, Pakistan, Oman, the United Arab Emirates, Qatar, Yemen, Djibouti, Saudi Arabia, Egypt, Greece, Italy and France. Several of the undersea cable’s landing stations are located where the PRC also has invested heavily in infrastructure it has or intends to militarize, such as in Djibouti, which faces a high risk of debt distress and where the PRC opened a naval base in 2017. “In Pakistan, the cable network will land in Gwadar, a port China is developing as part of Belt and Road and where U.S. officials believe Beijing wants to open a naval facility, which China has denied. The cable is planned to connect to a land-based link with China,” according to The Wall Street Journal. Several sections of the Asia-Africa-Europe cable experienced technical difficulties throughout 2021, BenarNews reported.

SOUTH CHINA SEA CONTEST

Perhaps nowhere are the security stakes higher than in the South China Sea. As the PRC has sought to seize control of the region through the construction and militarization of artificial islands, it has also begun laying undersea cables to expand its 5G networks and potentially increase its control of data flowing to nearby Southeast Asian countries, according to analysts.

The PRC has been spotted laying cables in the South China Sea on several instances. In 2020, using commercial satellite imagery, Radio Free Asia (RFA) and BenarNews documented such activities in the Paracel Islands, which are claimed by Taiwan and Vietnam. In 2017, China Telecom laid fiber-optic cables in the Spratly Islands between Fiery Cross, Subi and Mischief reefs, state media reported. The PRC was also observed laying underwater cables in 2016 to connect the city and military base at Woody Island to the PRC’s

island of Hainan, Reuters reported. The People’s Liberation Army has operated its own cable-laying ships since 2015, RFA reported.

Vietnam objected to the PRC’s cable activities in the Paracels in June 2020. “Vietnam has sufficient historical evidence and legal grounds affirming its sovereignty over the Hoang Sa (Paracel) and Truong Sa (Spratly) archipelagoes in accordance with international law,” Foreign Ministry spokeswoman Le Thi Thu Hang told reporters, according to the state-run Vietnam News Agency. “Therefore, any activity relating to the two archipelagoes conducted without Vietnam’s permission are violations of its sovereignty and of no value,” she said.

The fiber-optic connections between such Chinese-occupied features are likely meant for military purposes, James Kraska, a professor at the U.S. Naval War College, told RFA. Kraska said the cables are probably for encrypted military communications between China’s various outposts and will connect to the undersea cable system already installed along the PRC’s east coast.

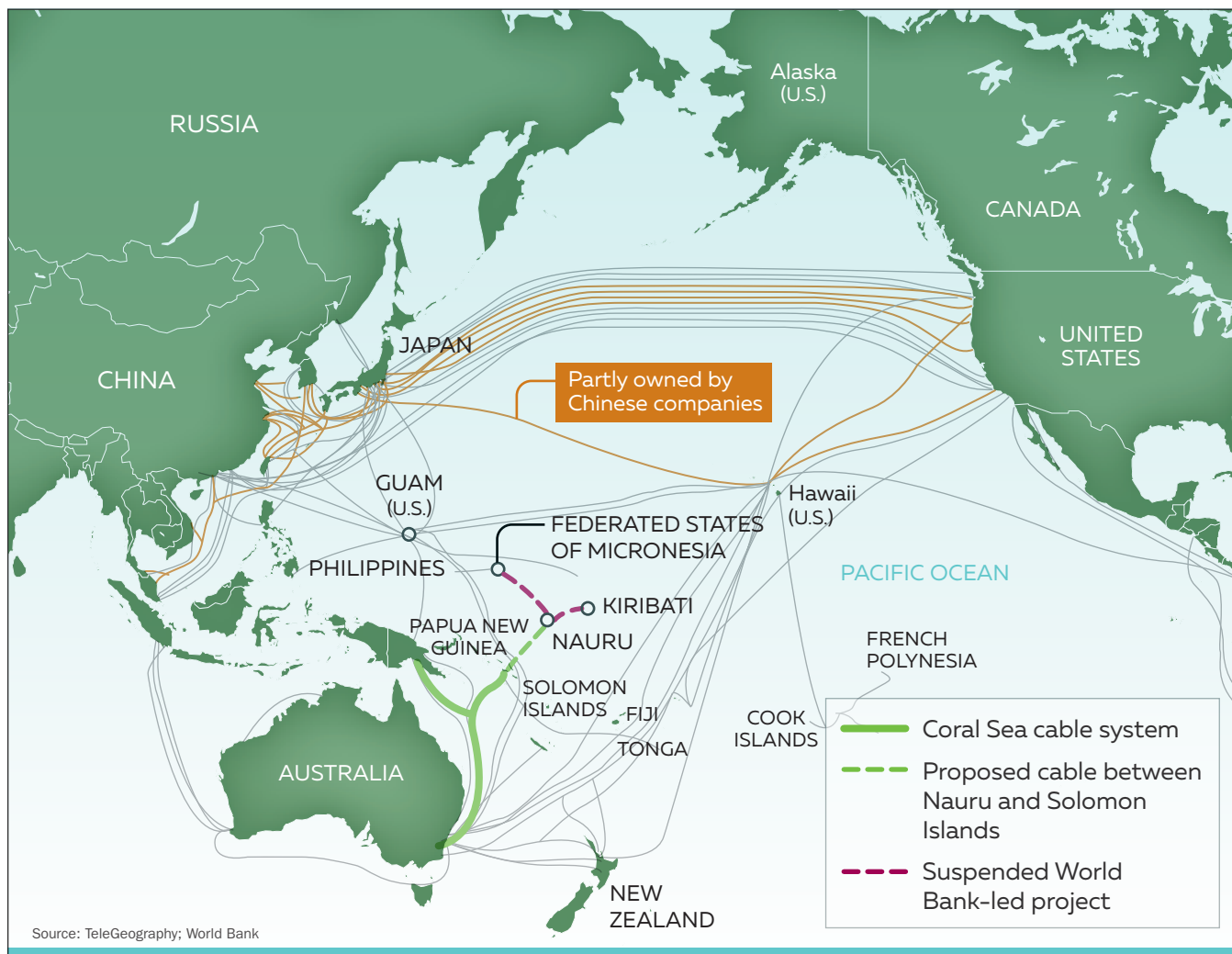
PRC control of emerging undersea networks in the South China Sea could enhance its grip on the region in the longer term, analysts warn. “The danger with China’s case, however, is the way they are attempting to circumvent international regulations and norms. By annexing islands in the South China Sea, they can claim that it is within their sovereign territory,” explained Helena Martin in a 2019 article in The McGill International Review, a daily online publication. International bodies would have less control of new cables if the PRC’s claims go unchallenged. The PRC “would technically be operating within their rights even though their operations would affect all of the Southeast Asian countries.” Violations of international regulations and norms through currency and market manipulation or even environmentally damaging practices would also be more difficult to sanction, Martin wrote.

Meanwhile, several commercial cable installations to connect Southeast Asia to the U.S., such as the Pacific Light Cable Network funded by Facebook and Alphabet, the parent company of Google, have also been delayed for security concerns. The line would have linked the Philippines, Taiwan and the U.S. with Hong Kong, which U.S. officials feared could provide sensitive global data to the PRC given its crackdown on the territory. A Facebook project to link California to Hong Kong was also scuttled in 2021 for the same reason.

Market dynamics may further complicate security issues as tech companies continue to look to Southeast Asian users for expansion. “Submarine cables go hand-in-hand with the exponential growth of cloud [computing] services,” Claude Achcar, managing partner of Actel Consulting, told Nikkei Asia in April 2021. “The smart thing for countries is not to pick sides. Indonesia and fellow ASEAN [Association of Southeast Asian Nations] nations are better off welcoming tech firms from both China and [the] U.S.,” Achcar said.

UNDERSEA CABLES IN THE PACIFIC

Nauru has turned to Australia to negotiate a new communications cable system after pulling out of a World Bank-led project over concerns a Chinese company would win the contract.



BALANCING ACT

The advantages of increasing access to broadband internet and the fast flow of information must be carefully weighed against security concerns for the long term, other analysts contend. “It’s really a matter of regret to see those geopolitics descending right down the stack into the physical layers of the internet,” Emily Taylor, a cyber policy analyst and fellow in security at Chatham House, told Bloomberg in March 2021. “What we’re all going to have to come to terms with is this: How do we try to keep as many doors open as we can without laying ourselves open to national security threats?”

As things stand, undersea cables will be entangled with security risks for the foreseeable future. For this reason, allies and partner nations must work with the

private sector to push for better intelligence sharing, risk assessments, security standards, monitoring and repair capabilities and contingency planning, and for stronger protections in international law to safeguard the world’s undersea cables and ensure their resilience, analysts recommend.

“As the White House increasingly focuses on cybersecurity threats to the nation and the global community, including from the Chinese and Russian governments, it must prioritize investing in the security and resilience of the physical infrastructure that underpins internet communication worldwide,” Sherman concluded in his Atlantic Council report. “Failing to do so will only leave these systems more vulnerable to espionage and to potential disruption that cuts off data flows and harms economic and national security.” □



Combating Health-Related CYBERSECURITY THREATS

What the Virtual World Can Learn from Public Health

DR. SEBASTIAN KEVANY AND DR. DEON CANYON/DANIEL K. INOUE ASIA-PACIFIC CENTER FOR SECURITY STUDIES

The cyberattacks on the Republic of Ireland's health system in May 2021 clearly show how the realms of cybersecurity and public health overlap. Hackers used an encryption process to disable the health system, paralyzing services and putting lives at risk when surgeries and other essential services had to be postponed.

The Irish government had to weigh the tradeoff between paying ransom to the hacking group versus risking the release of protected health information. A legal injunction against the use of the information, combined with public anti-ransom statements and a broader sense of public disgust and outrage, were effective tools against the hacking group, and the feared loss of private data or contamination of medical records was avoided.

The Irish experience reveals important global lessons: first, that health systems have to be protected by enhanced cybersecurity in the same way that banks and other key societal mechanisms do; second, health systems must be aware of the risks of increasingly relying on digital versus paper records; and third, many questions concerning the degree to which health information privacy can be maintained remain unanswered.

While cybersecurity and disinformation are distinct problems both in etiology and solution, internet regulation is a concept that embraces both issues. Likewise, the protection of personally identifiable information and protected health information are both virtual and tangible issues. Here, we attempt to draw these disparate and distinct concepts together in a framework that unites public health, health security and what might be termed cyber health.

THE CONTEMPORARY CYBER ENVIRONMENT

Contemporary cyber insecurity and unregulated internet have been described as the modern Wild West — a domain in which conventional rules, mandates and laws, even when they can be applied, are almost impossible to enforce.

The extremes of cyber freedom can be seen all around us — from verbal assaults and racism to enabling extremist positions on political and social issues, to the relative ease with which pharmaceuticals, pornography and other extreme or violent content can be accessed by any or all members of society with a web connection, regardless of age or educational level.

In turn, this collection of threats to society and public health presents a range of national and international security challenges. Currently, however, it seems highly unlikely that the transnational freedom of expression, trade and virtual movement that the internet represents will be controlled by any government or surveillance effort. In the absence of a national or supranational controlling body, the status quo looks set to continue: Even countries that enforce stricter national internet policies are inevitably exposed at the international level and circumnavigated by the global and nonconformist nature of cyberspace.

Yet nations need to balance cyber freedoms with health and security threats. Extreme cyber freedom can foster misinformation and even growth of extremist and terrorist organizations. However, censorship and internet controls create their own set of security and health threats, not least because they can advance the power and control of authoritarian regimes.

Many, if not all, of the above issues can be classified as global public health threats as well as security threats; virtually every crisis is accompanied by impacts on health. There may, therefore, be opportunities for a concerted public health response to cyber extremism as part of a broader national and international response to the issue.

THE UNIQUE CYBER HEALTH NEXUS

Health systems are particularly vulnerable to hacking, partly because of the sensitivity of the information and its potential ransom value. In 2020, the research organization Becker Health

revealed that 82% of the United States hospitals surveyed experienced a cybersecurity incident in the past year, even though health care-related cyber incidents account for only 1.5% of data breaches. However, the average cost per breached record was U.S. \$408, which is two to five times the cost in other industries.

Further, Verizon's "2021 Data Breach Investigations Report" shows that 2.2% (655) of all reported incidents and 9% (472) of all reported data breaches worldwide occurred in the health care industry. Also, the origin of threat actors behind these attacks has shifted from 2019, when actors were predominantly internal, to a level of 61% external attacks. The motivation behind these attacks was described by perpetrators as 93% financial; 3% fun; 2% espionage; 1% grudge; and 1% convenience. Relatedly, cyberattack sophistication on health systems is also increasing, with hackers now able to modify medical records and even imaging scans in addition to stealing them.

There are three main causes of losses of confidential information in the cyber environment: malicious and criminal attacks account for 48% of all data breaches, followed by human error at 27%, and system errors at 25%. Cyber incidents in health care organizations also have a more pronounced impact on customers and patients, who are more likely to bring class-action lawsuits and take their business elsewhere than in other contexts.

In response, there can be significant costs to health care institutions as they face requirements to update software or replace entire networks. Of note in this context, some attacks, such as the 2017 WannaCry ransomware sponsored by North Korea, targeted medical devices as well as health services.

More specific motivations may drive future cyberattacks. Cyber assassinations are now theoretically possible as hackers could cease airflow to a patient or ward, prevent patients from being moved to urgent

surgery by disabling elevators, modify patient scans to initiate emergency surgery, or alter the function of lifesaving medical devices. Motivations behind terrorist or state-sponsored attacks would likely include market manipulation, by targeting large health care organizations and the theft of intellectual property.

PUBLIC HEALTH AND CYBER HEALTH PARALLELS

During the COVID-19 pandemic in 2020, cyberattacks against health care-related organizations doubled, with 28% tied to ransomware. Phishing attacks were considered a high risk threat, according to a 2021 CrowdStrike report on global threats, with tactics including: exploitation of individuals seeking information on disease tracking, testing and treatment; impersonation of medical agencies requesting information, including the World Health Organization (WHO) and the U.S. Centers for Disease Control and Prevention; and offers of financial assistance or government stimulus packages in exchange for private information.

As noted above, internet regulation is distinct from cybersecurity, and can also separately and distinctly contribute to misinformation in public health. Yet with the generalized failure of most internet regulation efforts, the internet has been used to amplify misinformation and disinformation in the public health realms, as most recently represented by vaccine conspiracy theories and associated pseudo-science. Even if it were enforceable, or means to regulate such malign activity could be devised, internet regulation is insufficient to address the problem.

In the public health and cyber realms, much of the nomenclature is the same: viruses, scans, bugs and other cybersecurity terms have all been appropriated from the medical arena. Similarly, cyber threats have much in common with infectious disease threats, often following the same cyclical arcs of acceleration and tapering, as seen in epidemics. Further, the global nature of cyber and public health considerations is now clear. There may, therefore, be much to learn from public health's responses to epidemic infectious diseases and viruses to help with conceptualizing cyber threat responses.

A SOLUTION FROM WITHIN PUBLIC HEALTH?

Public health campaigns have a history of success. Whether it is prevention messaging regarding HIV/AIDS; health education regarding sexually transmitted diseases, malaria or tuberculosis; or the declarations of primary health care accords such as Alma Ata, global health has been inestimably improved by the efforts of organizations such as the WHO; the World Bank; the United Nations program on AIDS; the Global Fund to Fight AIDS, Tuberculosis and Malaria; and bilateral initiatives, such as the U.S. President's Emergency Plan for AIDS Relief.

Integrating cyber awareness messages into public health campaigns, and vice versa, may therefore be a meaningful way of educating the public about the perils



Authorities credited British information technology expert Marcus Hutchins with slowing the WannaCry global cyberattack in 2017 that held computer files hostage, including those of the National Health Service in the United Kingdom. THE ASSOCIATED PRESS



and disinformation readily available in cyberspace. Related policy recommendations might include:

- Health campaigns for HIV/AIDS and other infectious diseases could be expanded to include warnings about online disinformation regarding treatment and prevention. Such indirect approaches may result in improved health and cyber awareness in many developing countries, with citizens being encouraged, in health as in other realms, not to trust everything they read online.
- There may be scope for more direct involvement by the WHO and other U.N. organizations to combat general misinformation in cyberspace. This might include policies and messaging campaigns that warn against internet “facts” and “fake news” in such realms as extremism and terrorism, or in regard to public mental or physical health.
- The primacy of internet privacy should be reviewed when balanced against the functioning of health systems, ransom requests and hacking threats. The reality that we all, daily, trade personal privacy for the many instant benefits of internet use may mean that personal data privacy can no longer be held sacrosanct. Likewise, a reduced emphasis on data privacy will have significant potential benefits in preventing and containing future epidemics through ease in data sharing and tracking vectors in real time.
- Many of the apps, organizations and companies that allow for untraceable hacking are based in the U.S. and Europe. Some of these, such as the

Tor Onion Project, allow hackers to operate freely and anonymously during ransom efforts. Though these apps are framed as ways of allowing free and anonymous communication by dissident journalists and other noble causes via the internet, they also facilitate many dark web activities such as ransom, hacking, and human and arms trading. It may be necessary to review policies that allow for such criminal activities.

- Technology-based solutions to cybersecurity issues are now essential. These include administrative, physical and technical protection of sensitive personal and health information and tighter national and international internet regulation to address internet-based misinformation.
- Leadership prioritization of cybersecurity as an information technology problem in health care must change. This has rapidly become a patient-care threat that requires an enterprise risk management approach.

Controlling rampant cyber threats will take time — but with a multisector response employing the resources of all relevant organizations, progress can be made in bringing both a thrilling and a dark era of extreme cyber liberty to a close. We have learned that threats to personal health are taken seriously when presented by senior national and international health officials: there is no reason why the same set of principles should not be applied to the expanding cybersecurity threat and its nexus with global health. □

This article originally was published in the July 2021 edition of the Daniel K. Inouye Asia-Pacific Center for Security Studies' online journal Security Nexus. It has been edited to fit FORUM's format.



Thai Researchers Develop Robotic System to **SQUEEZE OUT MORE VACCINE DOSES**

Researchers in Thailand have developed a machine to draw out COVID-19 vaccine doses more efficiently and optimize supplies.

Using a robotic arm, the AutoVacc system can draw 12 doses of the AstraZeneca vaccine from a vial in four minutes, according to the Chulalongkorn University researchers.

That is up 20% from the standard 10 doses drawn manually, they said. The machine only works on AstraZeneca multidose vials.

“The extra 20% that we get means that if we have AstraZeneca for 1 million people, this machine can increase the number of doses to 1.2 million people,” lead researcher Juthamas Ratanavaraporn said.

While some health workers can draw up to 12 doses per vial using syringes designed to reduce waste, it requires a high level of skill, Juthamas said. “This could drain a lot of the health workers’ energy. They would have to do this every day for many months.”

Through September 2021, about 9% of Thailand’s more than 66 million people had been fully vaccinated, with the rollout hindered by lower-than-anticipated vaccine supplies.

The research team said it should be able to produce 20 more AutoVacc units within three or four months but that government funds and support would be needed to expand nationwide.

The prototype machine costs 2.5 million baht (U.S. \$76,243), including associated materials such as syringes, Juthamas said. The researchers also plan to make similar machines to use with the Pfizer-BioNTech and Moderna vaccines, she added.

Juthamas said the machines will ease the burden on health workers. “When the health workers are too tired, there are also chances of human error, so we should let the machines work on this,” she said.

Reuters

Mystery of Space

Inspired New Zealand Rocket Man’s Journey to Nasdaq

New Zealand entrepreneur Peter Beck, pictured, said his space firm, Rocket Lab, is the result of a lifelong quest for signs of life beyond Earth, as the startup hit a new milestone with a Nasdaq listing in late August 2021.

The satellite launch firm, often compared to Tesla Inc. CEO Elon Musk’s SpaceX, listed on the Nasdaq Composite with a market capitalization of about U.S. \$4.4 billion.

Rocket Lab agreed in March 2021 to go public through a merger with a firm backed by private equity firm Vector Capital, the latest in a series of space firm listings involving special purpose acquisition companies.

“For me personally, the biggest question that I can possibly answer in my lifetime, and the biggest question for everybody on Earth really, comes down to are we the only life in the universe or not,” Beck said.

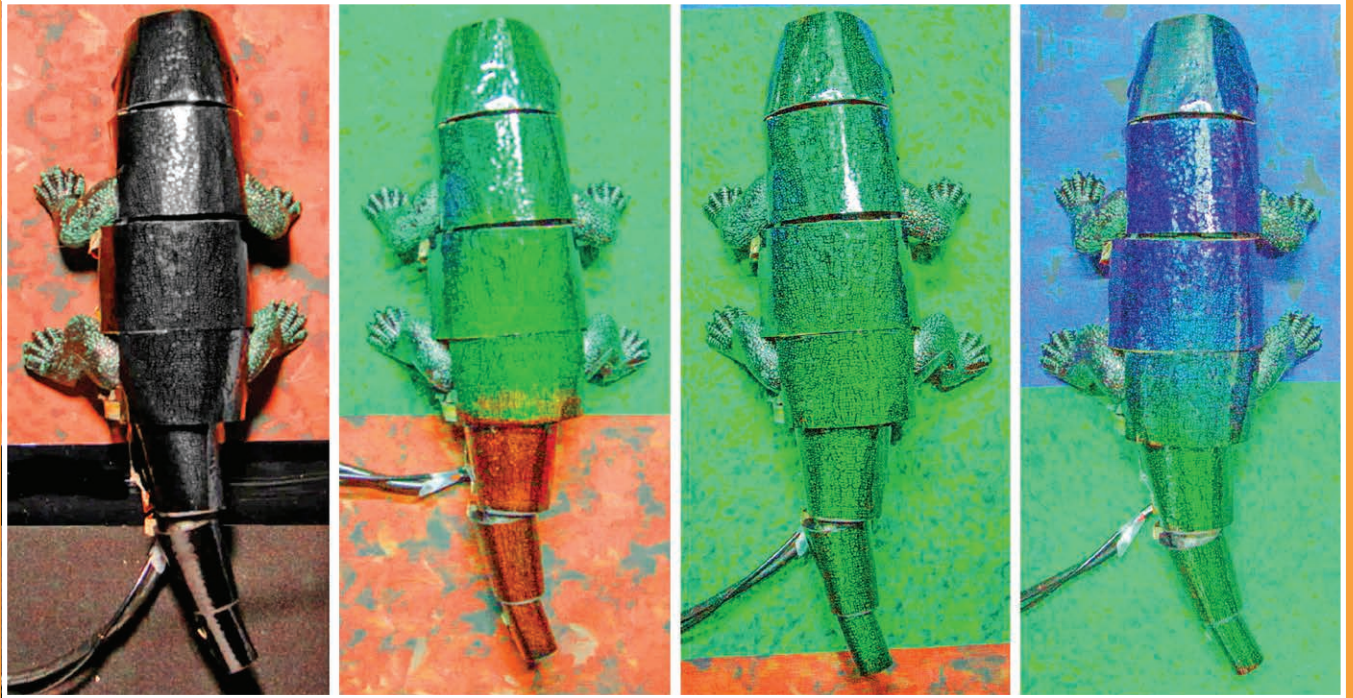
Growing up in Invercargill, a city near the southern tip of New Zealand’s South Island, he got interested in space when his father pointed to the stars and said there could be someone watching him from there. “That was the most mind-blowing moment in my young life. So I promised myself that if I ever had the chance to answer the question, which is fundamentally important to the way we think, I would have a crack. I am pleased to have this opportunity. We have spacecraft, launch pads and the team to do it.”

Rocket Lab was selected in 2021 to develop a spacecraft for a NASA mission to Mars. The company is also leading a private mission to Venus in 2023, working with a science team that discovered a gas called phosphine in the clouds of Venus in 2020.

“It’s a life-finding mission, it’s a high-risk mission and the very first private mission to another planet,” Beck said.

Rocket Lab, whose backers have included defense giant Lockheed Martin Corp., has launched over 100 satellites into space since 2006. Reuters





SOUTH KOREAN RESEARCHERS CREATE CHAMELEON-LIKE ARTIFICIAL ‘SKIN’

South Korean researchers have developed an artificial skin-like material, inspired by natural biology, that can quickly adjust its hues to match its surroundings like a chameleon.

The team, led by Ko Seung-hwan, pictured, a mechanical engineering professor at Seoul National University, created the “skin” with a special ink that changes color based on temperature and is controlled by tiny, flexible heaters. Their research appeared in the journal *Nature Communications* in August 2021.

“If you wear woodland camouflage uniforms in desert, you can be easily exposed,” Ko said. “Changing colors and patterns actively in accordance with surroundings is key to the camouflage technology that we created.”

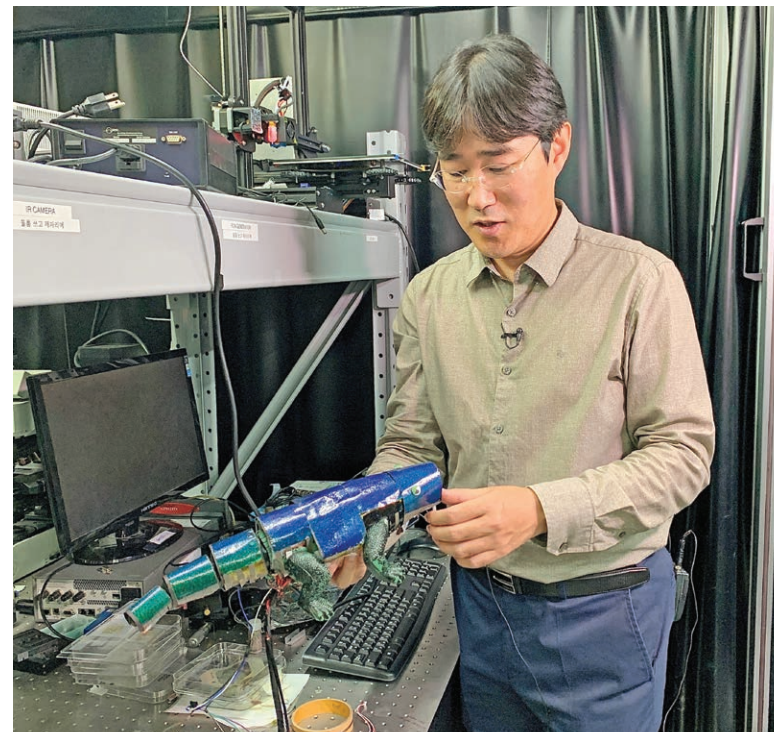
The team demonstrated the technology — thermochromic liquid crystal ink and vertically stacked multilayer silver nanowire heaters — using a robot with color-detecting sensors. Whatever colors the sensors “saw” around it, the skin tried to mimic.

“The color information detected by sensors is transferred to a microprocessor and then to silver nanowire heaters. Once the heaters reach a certain temperature, the thermochromic liquid crystal layer changes its color,” Ko said.

The flexible, multilayered artificial skin is thinner than a human hair. By adding silver nanowire layers in simple shapes such as dots, lines or squares, the skin can create complex patterns.

“The flexible skin can be developed as a wearable device and used for fashion, military camouflage uniforms, exterior of cars and buildings for aesthetic purposes and for future display technology,” Ko said.

Reuters



RESEARCHERS CREATE FIRST DETAILED MAP OF GLOBAL CORAL

STORY AND PHOTOS BY THE ASSOCIATED PRESS

Researchers have completed a comprehensive online map of the world's coral reefs by using more than 2 million satellite images from across the globe.

The new atlas will act as a reference for reef conservation, marine planning and coral science as researchers try to save these fragile ecosystems that are being lost to climate change.

Named the Allen Coral Atlas after late Microsoft co-founder Paul Allen and completed in September 2021, the global, high-resolution map is the first of its kind. It provides detailed information about local reefs, including types of submarine structure such as sand, rocks, seagrass and, of course, coral.

The maps, which include areas up to 15 meters deep, are being used to inform policy decisions about marine protected areas, spatial planning for infrastructure such as docks and seawalls and coral restoration projects.

"Our biggest contribution in this achievement is that we have a uniform mapping of the entire coral reef biome," said Greg Asner, the project's managing director and director of Arizona State University's Center for Global Discovery and Conservation Science.

Asner said a network of hundreds of field contributors provided information about reefs so that researchers could program their satellites and software to focus on the right areas. "And that lets us bring the playing field up to a level where decisions can be made at a bigger scale because so far decisions have been super localized," Asner said. "If you don't know what you've got more uniformly, how would the U.N. [United Nations] ever play a real role? How would a government that has an archipelago with 500 islands make a uniform decision?"

The atlas includes a coral bleaching monitor to check for corals that are stressed due to global warming and other factors. Asner said about 75% of the world's reefs had not previously been mapped in such detail and many not at all.

The project began in 2017 when Allen's philanthropic foundation, Vulcan Inc., was working with Ruth Gates, a Hawaii researcher whose idea of creating "super coral," a species that can survive extreme conditions, for reef restoration was funded by



The Great Barrier Reef stretches more than 2,300 kilometers along Australia's northeastern coast and is home to over 9,000 species. The new atlas will help researchers monitor the health of coral reefs, including the world's largest.

INSET: Greg Asner, managing director of the Allen Coral Atlas and director of Arizona State University's Center for Global Discovery and Conservation Science, reviews ocean temperature data at his lab near Captain Cook, Hawaii.

Vulcan. Gates and Vulcan brought in Asner because of his work with the Global Airborne Observatory, which was mapping reefs in Hawaii at the time.

Allen, who said he wanted to help save the world's coral reefs, liked the idea of using technology to visualize data, so Gates connected the group with the satellite company Planet, and Allen funded the project for about U.S. \$9 million.

The University of Queensland in Australia used artificial intelligence technology and local reference data to generate the layers on the atlas. The maps can be viewed online.

Allen and Gates died in 2018, leaving Asner and others to carry on the work. "Ruth would be so pleased, wouldn't she?" Asner said. "She would just be tickled that this is really happening." He said a third of the calls he gets are from researchers hoping to use the maps to "be sure that their planning and their reef restoration work is going to have its max efficacy."

When Gates found out she was sick, she selected friend and colleague Helen Fox from the National Geographic Society to help conservation groups use the tool. "It really was a global effort," said Fox, who is now the conservation science director for Coral Reef Alliance. "There were huge efforts in terms of outreach and helping people be aware of the tool and the potential scientific and conservation value."

aerial COMBAT



Republic of Korea 2nd Army Soldiers perform high-flying maneuvers during a taekwondo demonstration for visiting U.S. Secretary of Defense Lloyd Austin and South Korean Defense Minister Suh Wook at the Ministry of National Defense in Seoul in December 2021.

Photo by: Song Kyung-Seok/AFP/Getty Images

RELEVANT. REVEALING. ONLINE.

www.ipdefenseforum.com

Indo-Pacific Defense FORUM is provided FREE to military and security professionals in the Indo-Pacific region.

JOIN US ON FACEBOOK, TWITTER, INSTAGRAM,
WHATSAPP: @IPDEFENSEFORUM AND
LINE: @330WUYNT



All platforms may not be available at every location.

FREE MAGAZINE SUBSCRIPTION

FOR A FREE MAGAZINE SUBSCRIPTION:

www.ipdefenseforum.com/subscribe

write: IPD FORUM Program Manager
HQ USINDOPACOM, Box 64013
Camp H.M. Smith, HI
96861-4013 USA

PLEASE INCLUDE:

- ▶ Name
- ▶ Occupation
- ▶ Title or rank
- ▶ Mailing address
- ▶ Email address

DOWNLOAD
OUR APP!



NEW
CONTENT
POSTED
DAILY!

