INDO-PACIFIC DEFENSE

VOLUME 51, ISSUE 3, 2026

FORUM

STEALTH APPROACH

Allies, Partners Project Power in All Dimensions

PLUS

Countering Cyber and Information Threats

Asymmetric Advantages

features

departments

FORUM UNVEILS EXCLUSIVE DIGITAL FORMAT

Indo-Pacific Defense FORUM is moving to a fully digital format. This edition marks the final print issue of FORUM magazine, which will continue to feature in-depth analysis and perspectives online in 10 languages. You also can access exclusive content daily and magazine archives at ipdefenseforum.com.

We're honored to have served our readers for more than 50 years and remain committed to fostering dialogue on regional security issues.

Thank you for your continued support.

ABOUT THE COVER
Multilateral partnerships among Indo-Pacific Allies are creating an invisible shield of innovative solutions to protect the undersea domain and provide unrivaled advantages. FORUM ILLUSTRATION

Dear Readers,

This edition of Indo-Pacific Defense FORUM examines how the United States and its Allies and Partners are working together to attain asymmetric advantages over potential adversaries. The unrivaled coalition strives to maintain a decisive edge through innovation, integration of capabilities and strategies, and sustaining superior quality and readiness.

In the opening article, retired U.S. Army Col. James Minnich, a professor at the Daniel K. Inouye Asia-Pacific Center for Security Studies, details how the network of U.S., ally and partner components is conferring a strategic asymmetric advantage, citing Adm. Samuel J. Paparo, Commander of the U.S. Pacific Command. A supporting article by U.S. Army Col. Dave Butler, G37 Exercise Division director for the U.S. Army Pacific (USARPAC), highlights the critical role of USARPAC's Operation Pathways in reinforcing alliances and enhancing interoperability with key partners.

Next, Chris Mills, director of the University of New South Wales Defence Research Institute in Australia, explains why innovation is critical to ensuring deterrence for the U.S. and its Allies and Partners. Together they must create and implement superior capabilities sooner than adversaries, he writes, especially amid fast-moving advances in artificial intelligence and autonomous systems. A related FORUM staff article looks at how Indo-Pacific nations are innovating to address the mounting drone threat, including by creating layered defenses.

Writing about the cyber and information domains, Yeo Seow Peng, executive director of the Association of Southeast Asian Nations Defence Ministers' Meeting Cybersecurity and Information Centre of Excellence, chronicles how the Singapore-based entity is trailblazing initiatives to counter new threats. The center builds on regional capacity through exchanges and cooperation to boost trust and confidence. It also promotes information sharing among militaries and other defense entities.

Also in this issue, retired Republic of Korea Army Lt. Gen. In-bum Chun examines how the U.S. and its Allies and Partners are responding to the North Korean threat with a multidimensional approach. In addition to strengthening extended deterrence by enhancing cyber and financial resilience, maritime enforcement, and counter-special operations forces capabilities, Chun encourages Allies and Partners to remain vigilant in obstructing North Korea's cognitive coercion efforts.

We hope this edition elevates the discussion on the importance of alliances and partnerships for achieving asymmetric advantages in the Indo-Pacific.

Please contact the FORUM staff at **ipdf@ipdefenseforum.com** to continue the conversation and share your comments.

All the best,

FORUM Staff

IPD FORUM

Asymmetric Advantages

Volume 51, Issue 3, 2026

US PACOM LEADERSHIP

S.J. PAPARO
Admiral, USN
Commander

GEORGE B. ROWELL
Lieutenant General, USMC
Deputy Commander

ERIK J. ESLICH
Rear Admiral, USN
Director for Operations

CONTACT US

IPD FORUM

Indo-Pacific Defense FORUM
Program Manager
HQ US PACOM 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. 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 war has determined that the publication of this magazine is necessary for conducting public business as required by the Department of War.

ISSN 2333-1593 (print)
ISSN 2333-1607 (online)

RETIRED UNITED STATES ARMY COL. JAMES M. MINNICH is an academic and author with in-depth experience in Northeast Asia, including 15 years of duty in the Republic of Korea. He retired in 2019 after 37 years of active duty. Minnich has been a professor at the Daniel K. Inouye Asia-Pacific Center for Security Studies in Hawaii since 2016, previously serving as associate dean. He hosts and produces Dialogue, the center's online platform for critical discussions on Indo-Pacific security challenges. Featured on Page 8

CHRIS MILLS was appointed director of the University of New South Wales Defence Research Institute in Sydney, Australia, in August 2024. During more than 30 years in the Australian Army, he served overseas deployments and held roles including Joint Training and Exercises director, General Modernisation Army director, and General Force Options and Plans director. He has helped the Australian Defence Department develop workforce strategies and led delivery of the 20-year Defence Capability Plan and the 2020 Force Structure Plan. He also has consulted in defense, capability management and business transformation. Featured on Page 12

RETIRED REPUBLIC OF KOREA (ROK) ARMY LT. GEN. IN-BUM CHUN holds advisory roles for the National Bureau of Asian Research, the Korea Foundation, the Association of the United States Army and the Sweden-based Institute for Security and Development Policy. He served as director of U.S. affairs at the ROK National Defense Ministry and at all command levels, including the ROK Special Warfare Command. Featured on Page 20

U.S. ARMY COL. DAVE BUTLER serves as G37 Exercise Division director for the U.S. Army Pacific (USARPAC) and is the principal architect of Operation Pathways, an initiative to deploy combat-ready forces among Indo-Pacific Allies and Partners. He is responsible for planning and resourcing exercises, mission rehearsals, and other operations, activities and investments that advance USARPAC's positional advantage in the Indo-Pacific. He previously served as the division chief for the Geographic Combatant Command and Special Operations Division at the Joint Warfare Analysis Center in Virginia. Featured on Page 30

YEO SEOW PENG is executive director of the Association of Southeast Asian Nations Defence Ministers' Meeting Cybersecurity and Information Centre of Excellence in Singapore. She previously served as the Singapore Defence Ministry's director of international and regional policy. Featured on Page 32

U.S. MARINE CORPS LT. COL. KEVIN M. WHEELER is a nonresident fellow in the Indo-Pacific Security Initiative at the Atlantic Council's Scowcroft Center for Strategy and Security. He is operations officer and logistics integrator within the logistics division at Marine Forces Pacific in Hawaii. Previously, he was regimental logistics officer for the 3rd Marine Littoral Regiment, where he contributed to deterrence operations in the first island chain. His prior assignments range from tactical to strategic, with combat deployments focused on foreign force advisement and strengthening logistics supply chains.
Featured on Page 60

JAPAN TO DEPLOY
Missile Systems on Island Near Taiwan by 2031

A military radar station in Yonaguni, where Japan plans to deploy surface-to-air missiles by March 2031 GETTY IMAGES

Japan plans to deploy surface-to-air missiles by March 2031 on one of its remote western islands near Taiwan, the country's defense minister said in February 2026. It was the first time Tokyo has specified the timing of the deployment.

The Defense Ministry announced in 2022 that it planned to ramp up air defenses on Yonaguni, which hosts a Japan Self-Defense Forces base. The island is about 110 kilometers east of Taiwan, the self-governed island, and 1,900 kilometers southwest of Tokyo.

Japanese Prime Minister Sanae Takaichi told parliament in February 2026 that Japan needs to strengthen its defense capabilities in the face of intensifying attempts to change the status quo in the East China and South China seas.

Agence France-Presse

Australia Invests in Shipyard Infrastructure TO BOOST SUBMARINE ASSEMBLY

Australia will make a $2.76 billion down payment on a shipyard to help deliver nuclear-powered submarines under the trilateral AUKUS defense pact with the United Kingdom and the United States.

Announced in 2021, AUKUS is Australia's largest defense investment and will see U.S. Navy-commanded Virginia-class submarines based in Australia beginning in 2027. Australia will buy up to five of the submarines with delivery beginning in 2030 or later, and Canberra and London will build a new class of AUKUS nuclear-powered submarine.

Australian Prime Minister Anthony Albanese described the investment, announced in February 2026, as an initial payment to deliver the new shipyard in Osborne, a suburb of Adelaide in South Australia state.

"Investing in the submarine construction yard at Osborne is critical to delivering Australia's conventionally armed, nuclear-powered submarines," Albanese said.

He said the project is expected to cost about $21 billion over the coming decade.

The United States Navy Virginia-class submarine USS Minnesota arrives at HMAS Stirling in Western Australia in February 2025. LT. COREY TODD JONES/U.S. NAVY

Osborne is where Australia and the U.K. will jointly build Australia's fleet of nuclear-powered submarines, the core component of the AUKUS pact.

Reuters

India Joins Pax Silica Nations **to Secure Supply Chains**

Indian and United States officials celebrate after signing the Pax Silica agreement in New Delhi in February 2026.

India has joined a United States-led multinational initiative to strengthen technology cooperation among strategic allies in a move that underscores the countries' deepening ties.

The February 2026 decision aligns New Delhi with Washington's efforts to build secure supply chains for semiconductors, advanced manufacturing and critical technologies as geopolitical competition intensifies.

The Pax Silica framework also includes Australia, Israel, Japan, Qatar, the Republic of Korea, Singapore, the United Arab Emirates and the United Kingdom.

"Pax Silica will be a group of nations that believe technology should empower free people and free markets," said U.S. Ambassador to India Sergio Gor. "India's entry into Pax Silica isn't just symbolic. It's strategic. It's essential."

Launched in Washington in December 2025, the nonbinding coalition aims to enhance cooperation on semiconductor design, fabrication, research and supply chain resilience.

Availability and acquisition of rare-earth minerals essential to magnets and other advanced technology is an important provision. The initiative seeks to increase the independence of manufacturing hubs and production networks across strategic allies.

India imports a large share of its critical minerals, which constitutes a vulnerability, India Today magazine reported. Pax Silica provides diversification, offering access to resources, capital and technology. The Associated Press

Panama Takes Ports from Hong Kong Conglomerate

Panamanian maritime authorities took control of two ports on the Panama Canal from CK Hutchison in February 2026 after the Panamanian Supreme Court annulled the Hong Kong-based conglomerate's contracts to operate the ports.

"The Panama Maritime Authority has taken possession of its ports and guarantees the continuity of operations," ports director Max Florez said.

The 80-kilometer interoceanic waterway handles about 40% of the United States' container traffic and 5% of world trade.

In January 2026, the court declared as unconstitutional the contract that had allowed CK Hutchison to manage the ports of Balboa on the Pacific Ocean and Cristobal on the Atlantic Ocean since 1997.

Florez said an 18-month transition period began after the final ruling, with the ports being operated by two other companies before contracts are awarded under a new international tender.

The canal was built by the U.S., which operated it for a century before ceding control to Panama in 1999. Agence France-Presse

A container ship transits the Panama Canal in January 2026.
AFP/GETTY IMAGES

NETWORKED ASYMMETRY

ALLIES WIN ON TEMPO, GEOMETRY AND QUALITY

U.S. ARMY COL. (RET.) DR. JAMES M. MINNICH
DANIEL K. INOUYE ASIA-PACIFIC CENTER FOR SECURITY STUDIES

An Indonesian Soldier, right, and a United States Marine participate in a Super Garuda Shield drill in Indonesia in 2024.
CPL. MIGEL A. REYNOSA/U.S. MARINE CORPS

In April 2025, a new picture of coalition power emerged across the Philippine archipelago. During Exercise Balikatan, United States Marines positioned long-range anti-ship missile launchers in the northern islands of the Batanes. Simultaneously, U.S. Army High Mobility Artillery Rocket Systems (HIMARS) rolled into coastal firing positions on Palawan, hundreds of kilometers to the southwest. At sea, Japanese frigates integrated with Philippine and U.S. vessels near the contested Scarborough Shoal in the South China Sea.

None of these individual moves rivaled an adversary's mass. They did not have to. Together, they represented a different logic of power: networked asymmetry — the ability of Allies and Partners to impose cascading dilemmas through tempo, geometry and quality to offset an opponent's numerical advantage.

Adm. Samuel J. Paparo, Commander of U.S. Pacific Command (US PACOM), describes this unparalleled network of alliances and partnerships as the U.S.'s key strategic asymmetric advantage. For example, exercises that were once bilateral, such as Balikatan in the Philippines and Garuda Shield in Indonesia, have evolved into multilateral test beds for integrating advanced technologies, synchronizing multidomain operations and rehearsing high-end warfighting at an unprecedented scale.

In advancing the concept of networked asymmetry, the coalition's decisive edge lies in its ability to outpace, outposition and outadapt rivals by fusing innovation, geography and alliance architecture. This advantage rests on three interdependent pillars:

- **Tempo:** Sensing, deciding and acting faster than competitors to seize and maintain the initiative.
- **Geometry:** Dispersing and positioning forces across contested spaces to create a resilient and unpredictable posture.
- **Quality:** Sustaining innovation, interoperability and resilience to win the long-term contest of adaptation.

FASTER THAN THE ADVERSARY: THE TEMPO IMPERATIVE

In modern warfare, speed is critical, but tempo is decisive. Tempo, the rhythm of observing, orienting, deciding and acting faster than an opponent, determines who controls the initiative. In his 2025 posture statement, Adm. Paparo made this US PACOM's central objective: to "see, understand, decide, and act faster than any adversary," denying them the ability to achieve their objectives. Achieving this requires more than just faster platforms; it demands a resilient, coalitionwide command and control (C2) backbone that transforms shared information into synchronized action.

FROM KILL CHAIN TO KILL WEB

The traditional kill chain model of warfare is linear and fragile. A kill chain is the systematic process used to rapidly and accurately locate and destroy an enemy target. The chain fails if any single link — from sensor to shooter — is broken. In contrast, a kill web is a distributed, resilient multinode network. It spreads detection, decision-making

and engagement functions across redundant platforms and units. If one sensor is jammed or a C2 node degraded, others are positioned to carry the mission forward, ensuring continuity.

Balikatan 2025 demonstrated this concept. When U.S. Marines deployed the Navy-Marine Expeditionary Ship Interdiction System launchers to the Batanes Islands alongside their Philippine counterparts, they did more than position hardware. They integrated a sophisticated fires system into a combined sensing and fire-direction architecture. The subsequent simulated strikes demonstrated a fused coalition kill web's ability to move targeting data cleanly across national and service boundaries and to act on compressed timelines. The result is a powerful deterrent message: The alliance can generate combat effects at a speed no adversary can match. Adm. Paparo has called this "decision superiority" the ultimate tool to "reduce the risk of miscalculation."

INSTITUTIONALIZING TEMPO

For tempo to be a durable advantage beyond scripted exercises, coalitions must cultivate three core habits:

- **Shared Data and Delegated Authorities:** The heat of a crisis is not the time to negotiate information-sharing agreements. Coalitions must establish common data standards and prearranged release authorities that prevent bureaucratic bottlenecks at the most decisive moments.
- **Rehearsals Under Duress:** Drills must move beyond best-case scenarios. By routinely injecting degraded communications, cyber interference and split-command scenarios into training, forces normalize rapid recovery and build the muscle memory to operate in contested environments.
- **Trusted Automation with Humans in the Loop:** Leveraging artificial intelligence and machine-learning algorithms can drastically accelerate the processing of vast amounts of sensor data, presenting commanders with viable options in seconds, not hours. This is not about replacing human judgment but augmenting it to operate at machine speed.

When tempo becomes the baseline expectation, adversaries are forced to hesitate. That hesitation, born from uncertainty about the coalition's response time, is deterrence delivered at the speed of relevance.

SURVIVE BY DISPERSING: THE GEOMETRY OF UNCERTAINTY

Across the Indo-Pacific, distance and dispersion reward agility. Geometry transforms the region's geography from a challenge into a decisive advantage. Instead of concentrating forces in a few large, vulnerable hubs, this approach disperses combat power across a network of smaller, more resilient sites, profoundly complicating an adversary's surveillance and strike calculus.

Balikatan 2025 provided a master class in strategic geometry. The U.S. Army's maneuver of HIMARS launchers over 240 kilometers by land and sea to Palawan for a live-fire drill demonstrated the ability to project

precision firepower from unpredictable locations. This was complemented by Philippine Navy fast attack craft and Australian Javelin launch unit teams securing the littoral zone. Far to the north, the expeditionary fires base in the Batanes proved that potent effects can be staged from austere terrain in strategic choke points without relying on static, easily targetable infrastructure.

These actions exponentially multiplied the number of aimpoints an adversary would have to track and target, forcing them to expend finite intelligence, surveillance and reconnaissance (ISR) assets and munitions to cover a bewildering array of dilemmas.

TRANSLATING ACCESS INTO ADVANTAGE

This operational geometry is underwritten by forward-thinking diplomacy. A resilient network of interlocking pacts from the Philippines-U.S. Enhanced Defense Cooperation Agreement to the growing number of reciprocal access agreements linking key partners such as Australia, Japan, the Philippines and the Republic of Korea forms the foundation for this distributed posture. The agreements translate political commitments into operational options: the ability to rotate forces, pre-position critical supplies, and train together with greater frequency and realism. In this context, geometry is not about static basing but about gaining time: the critical hours and days dispersed units need to absorb a potential first strike, displace and continue the fight. The same distributed networks that move launchers and supplies for defense also enable a more rapid and resilient humanitarian response, saving lives in peacetime and preserving combat power in crisis.

This geometry forces adversaries into an unfavorable cost-exchange ratio, where they spend far more on ISR and munitions to find and neutralize a target than the defenders expend to remain mobile and viable. That economic friction is asymmetric advantage in its purest form.

WIN ON ENDURANCE: THE QUALITY OF ADAPTATION

In a protracted conflict, the ultimate advantage goes to the side that can endure, adapt and regenerate. For the

LEFT: A Navy-Marine Expeditionary Ship Interdiction System is off-loaded from an Army Maneuver Support Vessel (Light) in Hawaii in September 2025. LANCE CPL. NICHOLAS FIGUEROA/U.S. MARINE CORPS

A Japan Air Self-Defense Force F-2 fighter jet prepares to refuel from a U.S. Air Force KC-135 Stratotanker during Exercise Cope North in 2024. SENIOR AIRMAN ARICK DUFFEY/U.S. AIR FORCE

alliance network, quality is less about possessing the most exquisite platforms and more about the holistic blend of rapid innovation, seamless interoperability and resilient sustainment, allowing forces to outadapt a numerically superior rival over weeks, months and years.

INNOVATION THAT SCALES

Adaptability thrives at the tactical edge. In 2025, U.S. Army units in Luzon in the northern Philippines used expeditionary 3D printers to manufacture and deploy mobile drones, achieving their ISR and strike capabilities in days rather than the months or years typical of traditional procurement. This model, built on iterative upgrades, modular parts and commercial off-the-shelf sensors, reflects a crucial shift toward affordable mass. Loitering munitions, uncrewed surface and aerial systems, and modular sensor nodes provide commanders with low-cost options that can be deployed at scale. The value is not in their elegance but in their adaptability to operational timelines.

INTEROPERABILITY AS A WEAPON SYSTEM

The most decisive platform in the Indo-Pacific is not a ship or a plane, but the network of partnerships itself. When data formats cross national borders effortlessly, when gateways can fuse and translate disparate sensor feeds, and when release authorities are rehearsed, the alliance's many sensor grids and magazines are fused into a single, vast arsenal. Adm. Paparo's emphasis on a resilient command, control, communications, computers, cyber, intelligence, surveillance, reconnaissance and targeting architecture, known as C5ISRT, underscores this point. A shared network is the connective tissue that enables a dispersed force to fight as a cohesive whole.

SUSTAINING THE FIGHT FORWARD

Endurance is a function of logistics. A distributed force can only persist if supported by a correspondingly distributed sustainment network. Fuel bladders, spare parts and repair capacity must be pushed to the edge. Pre-positioning stocks through bilateral agreements, leveraging commercial transport and establishing regional repair nodes are essential for shortening vulnerable replenishment lines. Initiatives such as Philippine-U.S. pre-positioning programs and broader allied industrial efforts, including the U.S.-led Partnership for Indo-Pacific Industrial Resilience and the AUKUS security partnership among Australia, the United Kingdom and the U.S., are not just about efficiency. They also are strategic imperatives designed to build a codevelopment, coproduction and cosustainment ecosystem that can withstand the pressure of conflict. The ultimate metric of quality is throughput under stress — the speed at which systems can be repaired, replaced or upgraded to maintain combat power.

AN ENDURING ASYMMETRIC ADVANTAGE

The Indo-Pacific's competitive landscape demands a strategic approach that values ingenuity over sheer mass. As recent exercises demonstrate, networked asymmetry — the integrated application of tempo, geometry and quality — provides the U.S. and its Allies and Partners with a powerful and enduring counter to adversary scale.

The effect is cumulative and reinforcing. Hesitation is imposed by superior tempo. Dilemmas are created by unpredictable geometry. Endurance is enabled by superior and adaptive quality. Together, these dynamics create a defensive web so resilient, responsive and lethal that it fundamentally alters an adversary's risk calculus. This is the ultimate aim of networked asymmetry: to build an advantage so clear and credible that it makes deterrence effective and conflict unnecessary. □

INNOVATION

KEY TO INDO-PACIFIC DETERRENCE

CHRIS MILLS/UNIVERSITY OF NEW SOUTH WALES DEFENCE RESEARCH INSTITUTE

Allies and Partners must generate, test and field capabilities faster than adversaries

As strategic competition in the Indo-Pacific intensifies, Australia and the United States have converged on complementary approaches to deterrence. Australia's National Defence Strategy frames deterrence by denial as preventing an adversary from achieving its objectives by making aggression infeasible or prohibitively costly by posturing and deploying resilient, survivable and networked military capabilities so that any attack risks failure or unacceptable losses.

The U.S., meanwhile, coordinates diplomatic, informational, military and economic tools, often with Allies and Partners, to shape adversary calculus and dissuade hostile action. Both approaches stand in contrast to the traditional model of deterrence by punishment, which relies primarily on the threat of retaliation after aggression to impose costs.

Both approaches also depend on more than platforms and optimized force posture; they demand continuous innovation grounded in focused research, agile development and adaptive operational concepts. Deterrence through denial must be particularly dynamic, evolving alongside emerging threats, technologies and operational concepts. In a world increasingly shaped by autonomous systems, gray-zone tactics and rapid technological change, static defenses and legacy systems quickly become obsolete. The capacity to continually evolve enables the fielding of smarter, faster and more resilient capabilities that detect, disrupt and neutralize threats before they materialize.

Amid fast-moving advances in artificial intelligence (AI) and autonomous systems, innovation has become the prerequisite for credible deterrence in the Indo-Pacific, where sea-lanes and the undersea domain are central to competition. A decisive factor in achieving denial will be the capacity to sustain a persistent, uncrewed presence across vast ocean spaces using advanced drones, autonomous surface and undersea vessels, and other AI-enabled platforms, while also keeping critical sea-lanes and ports clear of mines and other hostile undersea systems. Sustaining this posture requires continuous technological development, agile acquisition, and the rapid fielding and integration of emerging capabilities to enable deterrence to remain adaptive and credible as threats evolve.

Mission Specialist Defender Mark IV remotely operated vehicles locate and neutralize underwater mines. PETTY OFFICER 1ST CLASS JUSTIN E. YARBOROUGH/ U.S. NAVY

The Orca extra-large uncrewed undersea vehicle being developed for the United States Navy will have a range of more than 12,000 kilometers. THE BOEING CO.

Since 2009, Australia's strategic posture has increasingly emphasized deterrence by denial, moving beyond a narrow focus on territorial defense toward a proactive, regionwide strategy. Yet, capability gaps persist. The U.S. concept of deterrence stresses a comprehensive strategy that aligns all instruments of national power and deepens collaboration with allies such as Australia. At the core of both approaches is a requirement that is often underprioritized: sustained investment in research, testing and evaluation. Innovation is not merely a string of projects; it also is an institutional capability. Australia's Advanced Strategic Capabilities Accelerator and the U.S. Defense Advanced Research Projects Agency (DARPA) exemplify this, enabling rapid prototyping, iterative development and operational trials, while treating failure as learning rather than waste. Because innovation is cumulative, it demands steady funding and tight coordination across government, industry and academia.

TIME MATTERS

In an era of sharpening strategic competition and rapid technological churn, timing is as decisive as capability. Systems that take a decade to field risk missing their strategic window, just as costly platforms can be outpaced by inexpensive countermeasures before they reach scale. Time-to-deploy and time-in-effect must be treated as core acquisition criteria. The practical response is a procurement model built for speed and iteration, including agile acquisition and flexible contracting to compress schedules and move usable capability to the field. In parallel, it also is critical to sustain the longer-horizon research that underwrites future overmatch. In short, deliver within two to five years while continuing to promote scientific investigation and innovation.

The U.S. pairs this timing discipline with a broad, well-resourced research and development architecture spanning federally funded and university-affiliated centers, and competitive grant programs, some of them open to Allies and Partners. This is backed up with substantial investment.

About 3% of Australia's defense budget went to innovation, science and technology in 2024. The Australian Defence Science and Universities Network seeks to strengthen defense-university-industry links, although it operates at a smaller scale and with less

A prototype of the Manta Ray uncrewed vehicle, which is being developed for the U.S. Navy, undergoes testing in 2024.
NORTHROP GRUMMAN

The Royal Australian Navy's domestically developed Ghost Shark will conduct intelligence, surveillance and reconnaissance. The first of the long-range autonomous undersea vehicles was delivered in early 2026. AUSTRALIAN DEFENCE DEPARTMENT

institutional depth than comparable U.S. mechanisms.

Innovation is not an end in itself, however, and delivers little advantage unless it can be scaled. Prototypes deter little unless they can be produced affordably and at volume, which is why cost-to-scale and industrial readiness are decisive. As a result, industries must design for manufacturability, leveraging modular architecture, digital engineering and commercial off-the-shelf components, while governments strengthen supply chain resilience and workforce development.

Canberra and Washington are grappling with the challenge of scaling innovation, including through procurement and budgeting reforms, accelerated deployment and increased industrial capacity. To achieve overmatch this decade, they must accelerate entry for nontraditional vendors, reform acquisition systems, embrace disruption, and invest in production lines and enabling technology to scale at pace.

INNOVATION AND MARITIME AUTONOMY

In the maritime-dominated Indo-Pacific, autonomy is emerging as a game changer. Undersea and air-dropped drones offer persistence, stealth and rapid deployment for surveillance, interdiction and area-denial missions. When combined with AI-enabled command and control (C2), these platforms can form layered defense networks that complicate adversary planning and enhance deterrence. The U.S. Navy's Orca extra-large uncrewed undersea vehicle (XLUUV) program and DARPA's Manta Ray initiative to develop UUVs illustrate the trajectory. Australia is progressing in parallel, committing about $1.1 billion to a domestically built Ghost Shark XLUUV fleet under a five-year contract with Anduril Australia, with initial systems expected later in 2026.

Other regional actors also are moving quickly as demand fuels UUV market growth. Taiwan aims to deploy smaller drones, known as the Huilong or Smart Dragon, potentially capable of launching torpedoes.

To deliver results in maritime autonomy, the defense industrial base must be reformed to enable continuous innovation and durable deterrence. Procurement systems must prioritize speed, scalability and collaboration with nontraditional vendors, streamlining contracting, and incentivizing prototyping and field experimentation. Allied collaboration also is essential. Partnerships such as AUKUS, which comprises Australia, the United Kingdom and the U.S., and the Quad, which comprises Australia, India, Japan and the U.S., can pool resources, share intelligence, and develop technologies in undersea warfare, cyber defense and space, provided doctrines, standards and objectives are aligned.

Frontier technologies such as quantum computing, directed energy, hypersonics and advanced biotech will continue to shape deterrence; as such, governments must support foundational research and create transition pathways, with ethical, legal and safety guardrails embedded by design.

Deterrence in the Indo-Pacific depends on making innovation a standing institution, not a periodic initiative or patchwork of programs. It demands a force that can continually generate, test and field adaptive capabilities faster than adversaries can respond, especially at sea, where autonomous, layered systems such as UUVs and AI-enabled C2 deliver persistent effects.

Meeting that bar requires three disciplines:

- **Time:** Prioritize capabilities deliverable in two to five years while safeguarding long-horizon science.
- **Scale and sovereignty:** Design for manufacturability, build production lines that can be surged, harden supply chains and expand the workforce.
- **System reform:** Promote agile acquisition, open pathways for nontraditional vendors, and shared ranges, data and standards.

Allied integration also must be engineered through shared trials and interoperable architecture. If partners cannot build and field faster than threats evolve, deterrence will erode. If they can, it will endure. In the Indo-Pacific theater, innovation is the deterrent. □

COUNTERATTACK

Allies and Partners integrate defensive systems to combat drones

FORUM STAFF

ACCELERATION AND AFFORDABILITY are key pillars of the uncrewed aerial vehicle (UAV) strategy for the United States and its Allies and Partners in the Indo-Pacific.

The U.S. amplified the strategy when Secretary of War Pete Hegseth created the Joint Interagency Task Force (JIATF) 401 in August 2025 to rapidly acquire and integrate defense systems to combat small UAVs. The counter-uncrewed aerial systems (C-UAS) capability targets drones lighter than 590 kilograms.

"The main measure of effectiveness we have … is to ensure rapid delivery of state-of-the-art, innovative capabilities into warfighters' hands to increase the lethality," U.S. Army Lt. Col. Paul Lushenko, the task force's chief strategist, said during a December 2025 War Room podcast from the U.S. Army College.

Four months after Hegseth's announcement, the U.S. Central Command (USCENTCOM) launched Task Force Scorpion Strike to deliver efficient and economical autonomous systems. Its first squadron of low-cost uncrewed combat attack systems (LUCAS) is based in the Middle East. The LUCAS is derived from reverse engineering Iranian Shahed-136 technology — the drone Tehran has deployed against Israel and Russia has used against Ukraine. "Equipping our skilled warfighters faster with cutting-edge drone capabilities showcases U.S. military innovation and strength, which deters bad actors," said U.S. Navy Adm. Brad Cooper, USCENTCOM commander.

The LUCAS can be launched from catapults, rockets, vehicles or the ground. The UAV is about 3 meters long with a 2.5-meter wingspan and its delta-wing design allows for long-range loitering. The U.S. deployed LUCAS operationally for the first time in the initial stages of the Operation Epic Fury conflict with Iran that began in February 2026.

The Department of War said in late 2025 that it wants to deploy over 300,000 small attack drones. The $1 billion

ABOVE: A United States Soldier readies a Ghost-X surveillance drone during exercises in Germany in February 2025. GETTY IMAGES

Countering UAVs requires layered defenses, including radar, radio frequency sensors, cameras, acoustic detectors, lasers and potentially nets to capture drones and protect sensitive areas, infrastructure and personnel.

initiative, known as Drone Dominance, aims to have tens of thousands of autonomous aerial vehicles in the hands of service members in 2026 with hundreds of thousands available in 2027.

UAVs mark the intersection of trends in military technology — the precise nature of weapons and the rise of robotics allowing remote-control drones capable of delivering a lethal payload with no risk to a pilot, the Australian Army Research Centre noted in August 2024. UAVs have altered the dynamics of military operations, offering tactical advantages and enhanced operational efficiency. They can be used for surveillance, reconnaissance and targeted strikes.

"The corollary to the importance of armies fielding UAS is that effective, layered and efficient counter-UAS capabilities are neither a luxury nor a concept to be explored as part of an abstract future force. They are a basic requirement for a land force to be suitable for operations on the modern battlefield," said the 2024 study "Protecting the Force from Uncrewed Aerial Systems," published by the Royal United Services Institute for Defence and Security Studies, a London-based think tank. "Without C-UAS capabilities, a force will be seen first, engaged more accurately, and ultimately defeated by an opposing force that successfully fields UAS and C-UAS capabilities at scale."

Countering UAVs requires layered defenses, including radar, radio frequency sensors, cameras, acoustic detectors, lasers and potentially nets to capture drones and protect sensitive areas, infrastructure and personnel. Nonkinetic tools, called soft-kills, include jamming, spoofing and signal takeover to disrupt navigation systems and disable UAVs. Kinetic, or hard-kill, tools include gun-based systems, interceptors and directed energy weapons such as lasers or high-power microwaves to destroy UAVs.

"The worst drone threat is the one you don't detect," Oleksandra Molloy, a senior lecturer in aviation at the University of New South Wales in Sydney, Australia, told FORUM. "The question is no longer just which counter-drone system Indo-Pacific countries should acquire but how quickly [they] can establish the commercial and military partnerships to rapidly and effectively keep up with the changing threat."

LESSONS FROM UKRAINE

Drone technology has revolutionized warfighting since the Russia-Ukraine war began in February 2022. Both countries' tactics include the widespread use of small UAS and C-UAS weapons. "It is a tactical and technological inflection point," the Hudson Institute, a U.S.-based think tank, said in November 2025. "The war's defining feature has become the mass deployment of cheap, disposable, and networked technologies — especially drones, loitering munitions, and small-scale electromagnetic warfare systems."

Mass production is vital. Ukraine's Defense Ministry said in September 2025 that more than 1 million drones were delivered to military units over the first eight months of the year with millions more expected in early 2026.

Ukraine also changed acquisition procedures and allowed front-line commanders to obtain drones directly from manufacturers, sometimes within five days, according to Defense One, a U.S.-based publication.

The U.S. approach is similar to what the Ukrainians have done, Emil Michael, U.S. undersecretary of war for research and development, said at an August 2025 forum in Washington, D.C. "They push down the innovation to a very small unit level. They've competed them on which drones work better. Then they give more financing to the ones that work better. So that's their model. Our model is going to be: Bring it down to the unit level, reduce the barriers, provide broad training grounds."

Attack drones upended the economics of war. In June 2025, Ukraine said it used more than 100 remotely piloted drones to strike five Russian air bases, hitting 41 aircraft, including strategic bombers, and causing damage estimated at $7 billion. Kyiv also has successfully deployed naval drones — surface and underwater vessels equipped with anti-ship missiles. Ukraine's maritime drones premiered in October 2022 when nine drones attacked Russia's Black Sea fleet in the Crimean port city of Sevastopol. Even without a conventional naval fleet, Kyiv pushed Russian forces out of the western Black Sea, destroying about 20 vessels in a display of an effective asymmetric tool in contested waters, the Hudson Institute said.

In December 2025, Ukraine used an underwater attack drone to penetrate the Russian defenses at Novorossiysk naval base on the Black Sea and to disable a submarine. The submarine had attacked Ukraine's critical infrastructure and energy grid, according to The National Interest, a U.S.-based publication.

AFFORDABILITY ISSUES

Countering UAVs can be expensive without investing in technology. Between November 2023 and January 2025, the U.S. Navy defeated 380 Houthi rebel attack drones

and ballistic and cruise missiles in the Red Sea by firing more than 160 artillery rounds and 200 missiles, including 20 SM-3 missiles that each cost up to $28 million, Stars and Stripes newspaper reported. The U.S. expenditures also included 120 SM-2s worth more than $2 million each and 60 SM-6s at about $4 million apiece.

"We cannot afford to shoot down cheap drones with $2 million missiles and we ourselves must be able to field large quantities of capable attack drones," Hegseth said in announcing the Drone Dominance initiative.

The artificial intelligence (AI)-enabled Merops interceptor drone, used by Poland, Romania and Ukraine to detect and destroy small UAVs, costs about $15,000. That is half the cost of the Iranian-designed Shahed drone used by Russian forces against Ukraine, Defense One reported. Polish, Romanian and U.S. Soldiers trained on the Merops system in November 2025.

"It can defeat the Shahed-type threats, but also it demonstrates our ability to place capabilities that are much cheaper than some of our other previous systems ... to ensure that we are able to build the capacity against" future airborne drone threats, said U.S. Army Brig. Gen. Curtis King, commanding general of the 10th Army Air and Missile Defense Command in Germany.

The C-UAS and accompanying offensive systems will support Allies and Partners, said U.S. Army Col. Christopher Hill, senior director of the Global Tactical Edge Acquisition Directorate. The next steps are to develop autonomous air- or ground-launched systems as "the offensive systems that we're going to use to create a dilemma for our adversaries," Hill said. "We're going to replicate the same processes there in the Pacific region in order to not only support our U.S. unit there, but also our international partners in Australia, in South Korea and in Japan, and other partners there in the region."

The U.S. military has tested expanding its drone operations in the Western Pacific, including Airmen, Marines and Sailors deploying UAVs across Japan. In October 2025, an MQ-9 Reaper launched and landed without a runway at Kadena Air Base, Japan. Kadena is 595 kilometers from Taiwan, making it the closest U.S. air base to the self-governed island.

ALLIES AND PARTNERS COUNTER DRONES

Indo-Pacific nations are innovating to address the drone threat, said Molloy, including devising layered shields "so hostile drones could be jammed, shot with high-powered microwaves or lasered out of the sky before they pose a threat."

Japan is investing in laser-based counter systems such as a prototype that uses an infrared camera to detect targets. In late 2025, Tokyo demonstrated a 100-kilowatt laser system that can burn through metal and shoot down small UAVs.

Taiwan, meanwhile, is seeking to establish an international drone alliance, the Taipei Times newspaper reported. The government-backed Taiwan Excellence Drone International Business Opportunities Alliance and the Polish Chamber of Unmanned Systems signed an agreement in December 2025 to develop a "non-China" supply chain for drones and to collaborate on key technologies, Taiwan Foreign Affairs Minister Lin Chia-lung said. The effort will give Taiwan and partners an advantage in talent, technology, applying AI and funding, he said.

A SeaShark 800 uncrewed surface vessel, measuring about 8 meters long, undergoes testing in Taiwan in June 2025. GETTY IMAGES

The Australian Defence Department is partnering with DroneShield, an Australian defense technology company, to develop counter drone technology. DroneShield's DroneGun Tactical, a long-range counter drone system, is pictured. AUSTRALIAN DEFENCE DEPARTMENT

Taiwan's Defense Ministry also announced a $312 million initiative to acquire 635 lightweight counter-drone systems capable of assuming control over, jamming and data spoofing hostile UAVs. Taipei also is exploring autonomous maritime vessels.

"Uncrewed boats or vehicles have played a very significant role in the Ukraine war," Chen Kuan-ting, who serves on the Taiwan parliament's defense committee, told the Reuters news service. "Uncrewed vehicles, whether they are boats or underwater vehicles, can effectively deter China because Taiwan is not the attacking side, we are the defending side."

The twin-engine SeaShark 800 motorboat, for example, can carry 1,200 kilograms of explosives and has a range of 500 kilometers. "We can create uncertainty," William Chen, chairman of the Taiwan-based drone manufacturer Thunder Tiger, told Reuters. "We can fill the Taiwan Strait with danger and risks. No one knows where these dangers could surface."

In the Philippines, the U.S. Marine Corps temporarily deployed a unit of drones to support maritime security in the South China Sea, the U.S. Naval Institute News reported in November 2025.

Australia provided additional drone training to 30 Philippine Coast Guard officers in late 2025 to improve maritime security capabilities. The training followed delivery of $36 million worth of aerial drones and associated training to the Coast Guard, the Australian Embassy in Manila said.

Canberra announced Project Land Acquisition and Next-generation Development 156 in 2025 to rapidly deliver drone-defeating technologies to the Australian Defence Force, with initial contracts worth $16.9 million issued to 11 vendors.

U.S. defense firm Anduril Industries opened a manufacturing facility in Sydney, Australia, in October 2025 for its Ghost Shark undersea drone. The fleet is to be delivered to the Royal Australian Navy under a $1.1 billion five-year contract.

For Indo-Pacific countries, it is "important that these systems become affordable, scalable and increasingly autonomous, so that defending against drones doesn't bankrupt the defender," Molloy said.

In South Korea, the U.S. activated a squadron of MQ-9 drones at its air base in Gunsan in September 2025. The long-range drones can conduct surveillance and attack missions, and could be deployed to surveil North Korea and monitor activities in the Yellow Sea, analysts say. Seoul also is seeking to deploy advanced counter-drone systems that pair radar with jamming technology to neutralize small drones.

Small UAS are "the defining threat of our time," U.S. Army Brig. Gen. Matt Ross, director of the JIATF 401, told reporters in December 2025. "Our formations must be able to detect, track, identify and defeat these systems anywhere on the planet," Ross said. "This requires us to layer our defenses by integrating sensors with kinetic and nonkinetic efforts and battle management systems into a responsive, interoperable network." □

Countering North Korea's Asymmetric Playbook

Allies and Partners Respond with Multidimensional Approach

LT. GEN. (RET.) IN-BUM CHUN/REPUBLIC OF KOREA ARMY

North Korea has depended on asymmetry for more than seven decades. Economically weak, diplomatically isolated and technologically constrained, Pyongyang tries to compensate with a web of coercive tools: nuclear weapons, ballistic missiles, cyber intrusions, special operations forces (SOF), political warfare, smuggling networks, and extensive urban and subterranean defenses. These capabilities do not stand alone. Under dictator Kim Jong Un, they have merged into an integrated playbook designed to deter attack, secure concessions and fracture cohesion among the United States and its Allies and Partners.

Communist movements historically rose to power by exploiting the grievances of the poor, the hungry and the ideologically impressionable. They understood political manipulation long before the term asymmetric warfare existed. For them, the human mind was the decisive battleground. North Korea is a direct heir to this tradition. Cognitive warfare remains its most enduring asymmetric weapon.

The U.S. and its Allies and Partners are responding with a multidimensional approach — fortifying extended deterrence, enhancing cyber and financial resilience, tightening maritime enforcement, strengthening counter-SOF capabilities, and preparing for urban combat. But the contest is long-term, and Pyongyang invests heavily and still seeks advantage in the cognitive domain.

Extended Deterrence and Missile Defense

The backbone of allied strategy remains credible U.S. extended deterrence, backed by visible strategic assets and integrated missile defense planning. After the 2013 adoption of the Tailored Deterrence Strategy, longtime allies the Republic of Korea (ROK) and the U.S. have repeatedly updated their posture to account for North Korea's nuclear and missile capabilities. Revisions, especially in 2023, placed renewed emphasis on nuclear consultation mechanisms, real-time data sharing, and closer integration of conventional and nuclear deterrence.

The resulting approach is concrete. The U.S. regularly deploys long-range bombers, including B-52s, B-1Bs and occasionally B-2s, over and around the Korean Peninsula to signal alliance resolve. ROK fighter jets routinely integrate with these aircraft during combined air missions. U.S. ballistic missile submarines also resumed port calls in South Korea in 2023 for the first time in decades, providing unmistakable reassurances of nuclear commitment.

Missile defense cooperation has intensified. The ROK's Kill Chain preemptive strike concept, air and missile defense, and nuclear deterrence doctrine form a national framework that is reinforced by Patriot PAC-3 missile systems, and Japanese and U.S. Aegis ballistic missile defense platforms. Since 2023, trilateral data sharing enables almost instantaneous detection and tracking of North Korean missile launches.

Exercises reflect this integration. In 2025, the trilateral Freedom Edge off South Korea's Jeju Island brought air, naval, cyber and missile defense components from Japan, the ROK and the U.S. into a combined scenario, demonstrating the ability to coordinate deterrence and crisis response across domains. These measures complicate Pyongyang's nuclear planning and reduce the regime's confidence in nuclear coercion.

Republic of Korea (ROK) and United States personnel train at Osan Air Base, South Korea, in November 2025. STAFF SGT. SARAH WILLIAMS/U.S. AIR FORCE

Cyberwarfare and Disrupting Revenue Streams

North Korea believes that cybercrime is central to its survival. State-sponsored hacking groups such as Andariel, Kimsuky and Lazarus steal intellectual property, disrupt critical systems and — most notably — generate revenue through cryptocurrency theft. North Korean cyber operators stole an estimated $4 billion from 2017 to 2025. Major heists in India, Japan and the Middle East demonstrate the hackers' reach.

Allies increasingly approach this not merely as cybercrime but also as a sanctions-evasion regime. The ROK and the U.S. have elevated cyber cooperation through information sharing, joint attribution of major attacks and coordinated law enforcement action. Japan participates in joint advisories and supports rapid sanctions designations against North Korea-linked cryptocurrency wallets and accounts.

Financial defenses are tightening across the region. Crypto exchanges in Australia, Japan and Southeast Asia have strengthened know-your-customer and anti-money-laundering standards, often after coordinated Japan-ROK-U.S. warnings. North Korean information technology (IT) workers posing as freelance developers have been exposed and expelled due to improved biometrics and network behavior analysis provided through joint intelligence channels. These efforts

◀ **ROK Marines and Sailors conduct a landing drill near Pohang, South Korea, in November 2025.** ZUMA PRESS WIRE/REUTERS

significantly increase operational risk for Pyongyang and constrain its ability to rapidly convert stolen cryptocurrency into usable foreign currency.

SOF, Provocations and Escalation Control

North Korea has one of the world's largest SOFs, trained for infiltration, sabotage, leadership targeting and disruption. The regime deliberately pairs these units with calibrated provocations: artillery exchanges, drone incursions, naval clashes and other gray-zone actions designed to test resolve and manipulate political timing. More recently, North Korea has expanded its role well beyond the Korean Peninsula. Under a 2024 strategic partnership treaty with Russia, Pyongyang deployed troops and technical personnel to assist Russia's war against Ukraine. These forces reportedly participated in operations in Russia's Kursk region and have used drones and reconnaissance teams in Ukraine.

An ROK tank fires during an exercise with the U.S. Army at Rodriguez Live Fire Complex, South Korea, in December 2025.
1ST LT. JONATHAN SAULS/U.S. ARMY

The ROK and the U.S. have strengthened border surveillance, improved coastal radar integration, and enhanced joint intelligence, surveillance and reconnaissance. Combined counter-infiltration exercises train forces for rapid reaction to SOF incursions, hostage scenarios and destabilization attempts. The alliance has also refined escalation-management protocols, giving leaders a range of precise response options to impose cost without triggering uncontrolled escalation. These measures counter Pyongyang's long-standing belief that it can strike, shock and retreat with impunity.

Sanctions Evasion, Smuggling, Maritime Pressure

North Korea's illicit networks are essential to regime survival. Bureau 39 oversees operations that include coal smuggling, petroleum transfers, arms sales, counterfeit currency and narcotics distribution. These activities, which violate United Nations Security Council resolutions targeting North Korea's weapons of mass destruction (WMD) programs, increasingly rely on ship-to-ship transfers in international waters, concealment of vessel identity and shell companies disguised within regional business hubs.

The U.S.-led Pacific Security Maritime Exchange has become a central platform for multilateral information sharing. Australia, Japan, and European and Southeast Asian partners contribute data on suspicious vessels, illicit cargo movements and maritime identity fraud. Interdictions have increased, and North Korea-linked vessels have been seized and auctioned.

Training and capacity building play an important role. Southeast Asian coast guards and Pacific island states receive assistance to improve boarding protocols, evidence collection and maritime domain awareness. This cooperation narrows Pyongyang's options and pushes it toward riskier criminal methods, particularly cyber theft.

Preparing for Urban, Subterranean Warfare

Any major conflict on the Korean Peninsula would occur in some of the world's densest urban terrain and in areas laced with hardened bunkers and tunnels built over decades. U.S. assessments note that North Korea maintains extensive underground networks designed to move troops and equipment undetected. Four major infiltration tunnels have been uncovered, but many more likely remain hidden.

Combined ROK-U.S. exercises increasingly incorporate subterranean scenarios using uncrewed systems, robotics and teams trained in chemical, biological, radiological and nuclear defense to map, breach and neutralize tunnel networks. Civil defense planning continues to evolve, reinforcing shelters, emergency communications and continuity of government systems. These measures signal readiness for any asymmetric scenario North Korea assumes it can exploit.

Ideology, Cognitive Warfare

While missiles and cyber tools draw headlines, the North's most prevalent asymmetric weapon is cognitive warfare. Juche, the official state ideology of North Korea, has evolved far beyond its origins as a doctrine of self-reliance. Under Kim, it functions as a political tool — an instrument designed to preserve regime power internally while shaping perceptions externally. Juche is fused with nuclear identity to portray North Korea as dignified, sovereign and morally justified in pursuing nuclear weapons. This framing is an attempt to influence foreign audiences, normalize North Korea's illegal nuclear weapons and cast the regime as a victim of great-power

hostility. The narrative aims to blur responsibility for crises, portraying missile tests as defensive reactions and international sanctions as illegitimate.

North Korea disseminates false and misleading information through state media, intelligence services and proxy media platforms that operate with plausible deniability. These untrue narratives are recycled through fringe websites, bot networks and social media content farms in Southeast Asia and Eastern Europe.

Researchers have documented the regime's use of covert assets — including IT workers operating under forged identities — to distribute propaganda, manipulate comment threads and seed fabricated narratives into English- and Korean-language online forums. Some foreign influencers echo North Korean messages knowingly. Others do so unwittingly when they repeat misleading content wrapped in pseudoscientific or academic language. The goal is not persuasion in the traditional sense; it is distortion and division. By attacking the credibility of democratic institutions, amplifying local grievances and injecting doubt about alliance intentions, Pyongyang tries to erode cohesion within South Korea, weaken trilateral cooperation and undermine the international consensus supporting sanctions.

North Korea's information operations intensify during times of potential domestic instability in allied nations, such as elections, trade disputes and historical controversies. These surges often coincide with the regime's missile tests or cyberattacks as part of a synchronized coercive strategy that blends physical provocation with information manipulation.

Allied responses rely on transparency and exposure. Japan, South Korea and the U.S. issue coordinated public statements that clearly attribute North Korea's actions, highlight manipulated narratives and reinforce the legitimacy of U.N. Security Council resolutions. Seoul and Washington also publish detailed reports on human rights abuses, illicit finance and cyber operations, creating a factual narrative that counters North Korean propaganda.

Still, the cognitive domain is where Pyongyang can achieve disproportionate effects at minimal cost. The U.S. and its Allies and Partners must do more in this respect.

Regional and Multilateral Contributions

Countering North Korea's asymmetric warfare requires a regional effort. Japan is deepening missile defense, expanding counterstrike capabilities and sharing real-time data with the ROK and the U.S. Southeast Asian nations increasingly enforce sanctions, monitor ports and airspace, and expose North Korean front companies. Australia, the European Union and NATO partners contribute through sanctions enforcement, cyber defense and maritime monitoring. The 2003 global Proliferation Security Initiative to prevent the trafficking of WMD and related materials continues to constrain the North's arms transfers by enabling rapid interdiction of suspicious shipments. These regional contributions close many of the gaps Pyongyang historically exploited.

ROK and U.S. forces conduct a live-fire drill in Pocheon, South Korea, in December 2025. ZUMA PRESS WIRE/REUTERS

Long-Term Strategic Competition

North Korea's asymmetric strategy — rooted in ideology, empowered by missiles and cyber tools, and sustained by smuggling and information manipulation — is designed to ensure regime survival without confronting the superior conventional capabilities of the U.S. and its Allies and Partners. Pyongyang's objective is clear: alter perceptions, weaken cohesion and shape the environment to the North's advantage.

The changing geopolitical environment adds complexity. Moscow has become increasingly reliant on North Korean artillery and ballistic missiles. In return, Pyongyang seeks advanced technologies, intelligence sharing and political cover at the U.N. Security Council. Meanwhile, Beijing, through trade, diplomatic protection and lax sanctions enforcement, subtlely shields North Korea from full economic isolation. For Pyongyang, these arrangements reduce the costs of its asymmetric actions. For the U.S. and its Allies and Partners, they underscore the need for sustained multilateral coordination.

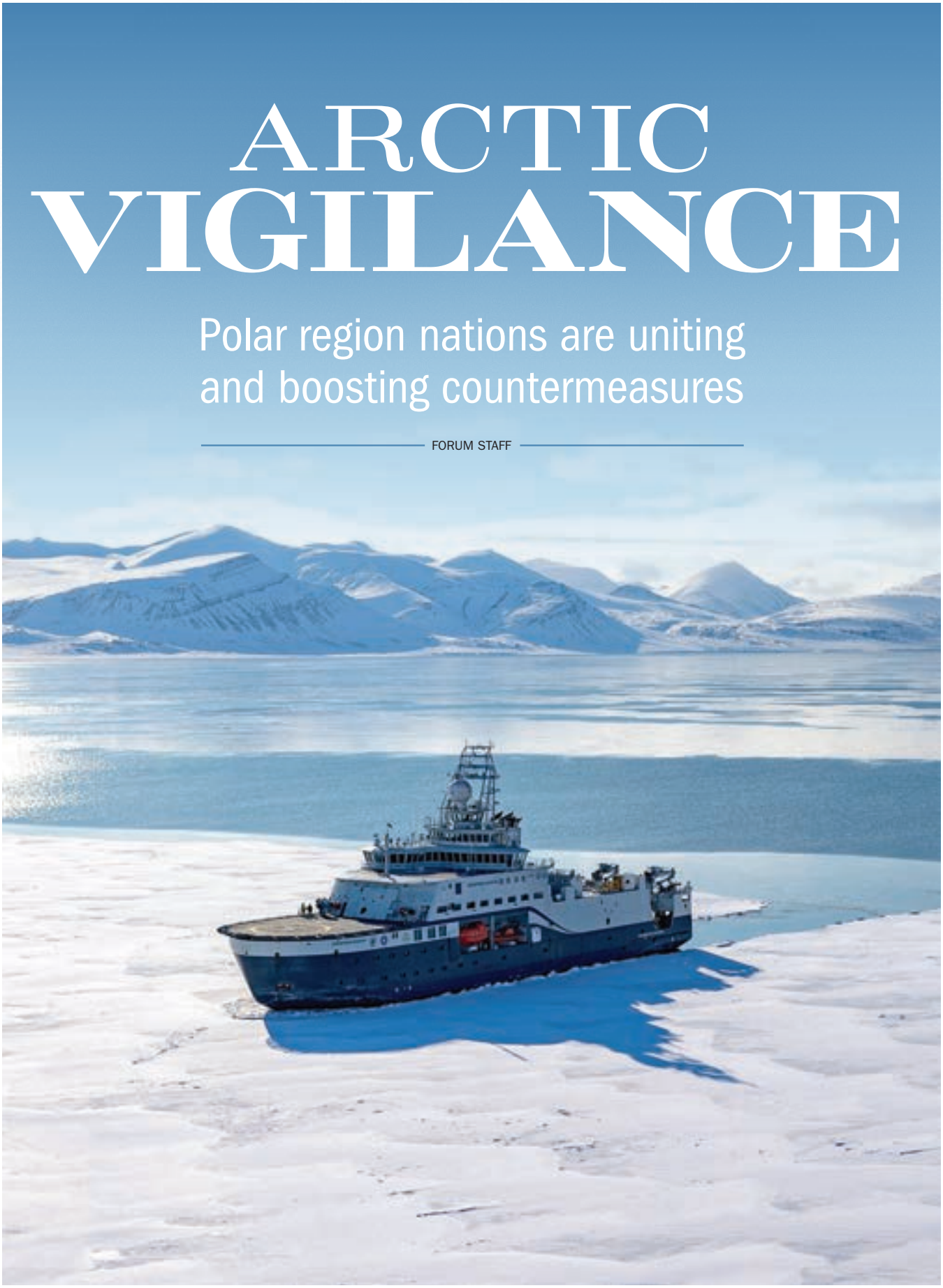
A second challenge lies within South Korea's information environment. North Korean cognitive warfare attempts to polarize South Koreans, exploiting generational divides and manipulating security narratives. Strengthening societal resilience through transparent communication, media literacy, consensus on national security and timely exposure of foreign disinformation has become as essential as strengthening air defenses.

The U.S. and its Allies and Partners are countering the North Korea challenge with a comprehensive response across military, informational, diplomatic and financial domains. Extended deterrence is stronger, cyber pressure is increasing, maritime enforcement is deeper and urban readiness is more mature. This is a long-term contest, and North Korea will continue adapting. But as allied coordination deepens, transparency increases and resilience grows, the space for North Korea's asymmetric advantage steadily narrows. The task now is to sustain this effort, refine it and ensure that the Indo-Pacific remains stable, secure and resistant to physical and cognitive coercion. □

ARCTIC VIGILANCE

Polar region nations are uniting and boosting countermeasures

FORUM STAFF



Deepening cooperation in law, scientific research and marine technology in the Arctic were highlights of a 2019 pact between China and Finland. The relationship, as it pertains to the polar region, has since cooled. The nations' 2025-2029 Joint Action Plan does not mention the Arctic.

When Finnish President Alexander Stubb visited Beijing in October 2024, mutual praise flowed at formal gatherings. But down-to-business meetings centered on Russia's war with Ukraine and Beijing's thinly veiled support of Moscow, a scenario that concerns Helsinki. Leaders ultimately approved measures on relatively benign issues such as trade, the environment and education.

The 2025-2029 strategy is just five pages, compared with the 30-page 2019 Sino-Finnish agreement that detailed joint initiatives in the region. "Overall, the focal points of the [Joint Action Plan] give an impression of shrinking cooperation," the Norway-based High North News newspaper reported in November 2024.

What happened? Most prominently, the Russia-Ukraine war began in February 2022, transforming the region's geopolitical and security environment. Amid concerns about its security, Finland, which has Europe's longest border with Russia (1,340 kilometers), joined NATO in April 2023, followed by neighboring Sweden in March 2024. Baltic Sea data cables, a gas pipeline and a power cable were severed, under suspicious circumstances, in 2023 and 2024 by commercial ships linked to China and Russia. The sea borders Denmark, Finland, Sweden and other European nations.

Other Arctic nations also became wary of China, which has served as Russia's High North proxy while the Kremlin wages its war with Ukraine. "The more China supports Russia, the more difficult the relationship with Europe, and especially the European Union, becomes," Stubb said.

In some respects, China still feels the fallout from its 2018 self-depiction as a "near-Arctic" state, a portrayal that rankled countries with territory inside the Arctic Circle. China's northern border is almost 1,500 kilometers outside the Arctic Circle.

All eight members of the multinational Arctic Council, a forum that promotes cooperation, coordination and interaction, initially were enthused about China's interest in the region. The forum includes Russia and seven NATO states: Canada, Denmark, Finland, Iceland, Norway, Sweden and the United States. China is among the Arctic Circle's 13 nonvoting observer nations, along with the Indo-Pacific countries of India, Japan, Singapore and South Korea.

Opinions about China among government officials and the public in the forum's NATO countries have spiraled downward in recent years, influenced by Beijing's increased links to Moscow, the nation with the most Arctic exposure, Trym Eiterjord, a Vancouver, Canada, researcher with The Arctic Institute, a Washington, D.C.-based think tank, told FORUM. "A lot of stuff has happened in the past year," Eiterjord said in December 2025. "A lot of it, at least when it comes to China, has been reactions from Arctic countries, from NATO countries."

Finnish President Alexander Stubb holds a news conference in Beijing in October 2024. THE ASSOCIATED PRESS

Many of China's forays into the Arctic — proposals to build power plants, airports and seaports in the extreme environment — have failed or remain on hold due to market factors, environmental hurdles, geopolitical challenges and security concerns. Its naval exercises with Russia trouble regional nations, as do Beijing's human rights abuses in places such as Tibet and Xinjiang, and its aggressive maritime actions in the Indo-Pacific.

The Sino-Russian naval exercises in the Arctic, and especially in international waters off Alaska's coast, might partly be swipes at the U.S., which has condemned China's hostile actions in the East China and South China seas, Eiterjord said. The U.S. and its Allies and Partners routinely transit the two seas to demonstrate freedom of navigation. Beijing illegally claims most of the South China Sea, where its Coast Guard ships have rammed, blocked and directed water cannons and lasers at other nations' fishing boats and

Norway's scientific research icebreaker RV Kronprins Haakon navigates sea ice near Spitsbergen, in the Svalbard archipelago, in April 2025. AFP/GETTY IMAGES

A 'NEAR-ARCTIC' STATE?

China's northern border is nearly 1,500 kilometers from the Arctic Circle

FORUM ILLUSTRATION

government vessels, particularly those of the Philippines. China also claims Japanese territory in the East China Sea.

China's Arctic explorations echo research missions and academic assessments that preceded Beijing's military expansion in the South China Sea, The Wall Street Journal newspaper reported in December 2025. China has built artificial features in the South China Sea that support military air bases.

Beijing has become less concerned about appearances in the Arctic. It no longer prioritizes impressing multilateral groups such as the Arctic Council. It now favors bilateral relations with Arctic nations and remains a key trade partner. Despite its remoteness, China has established a presence in the Arctic, using land-based research outposts and a fleet of oceanographic survey ships to explore sea topography, circumpolar features and space. It also participates in a regional group that opposes unregulated fishing, even though China's distant-water fishing fleet has been linked to such illicit activity globally.

Still, there's increasing skepticism about Beijing's intentions. "China's overtures have been met with suspicion in the Arctic states, where some analysts and commentators read nefarious intent into Chinese actions and statements," the U.S.-based Harvard Kennedy School's Belfer Center reported in June 2025. "China's construction of critical infrastructure and investments in the strategically located and resource-rich Arctic have raised concerns about national security. … What is more, questions abound about the dual-use applicability of Chinese research activities in the region."

COUNTERMEASURES

Finland is among the states enhancing asymmetrical defense capabilities in response to increased tensions. Expanding icebreaker fleets is part of that buildup. Canada, Finland and the U.S. in November 2025

A Danish Soldier sights a target during a NATO exercise in Greenland in September 2025. THE ASSOCIATED PRESS

celebrated advancement of their Icebreaker Collaboration Effort Pact. The endeavor aims to design, produce and maintain Arctic and polar icebreakers, as well as other capabilities — maritime operations for advanced navigation, remote sensing and environmental monitoring — by increasing information exchange, industrial collaboration and operational knowledge.

Finland, which will build icebreakers for Canadian and U.S. forces, has at least eight of the polar-capable ships, while Canada has 18 and the U.S. has three. China reportedly has five icebreakers and Russia more than 40.

Stubb and U.S. President Donald Trump reached a deal in October 2025 for Finland to build up to 11 icebreakers for the U.S. Coast Guard, with the initial four assembled in Finland and the remaining vessels built in U.S. shipyards using Finnish expertise.

Canada, which has built icebreakers for decades, has revitalized its shipbuilding industry and continues to work closely with shipbuilders and supply chains, Ottawa reported in December 2025.

Along with acquiring icebreakers, Canada will appoint an Arctic ambassador and open consulates in Anchorage, Alaska, and Nuuk, Greenland, Foreign Affairs Minister Anita Anand told the Reuters news agency in December 2025, adding that the Arctic is Canada's top foreign policy priority. Prime Minister Mark Carney plans to raise the defense budget to 5% of gross domestic product by 2035 as Canada prioritizes stronger international partnerships and an enhanced military.

"Canada is a sovereign nation, but that sovereignty is under new and growing pressures," Defence Minister David McGuinty said in May 2025. "As an Arctic nation, we must protect our northernmost regions and strengthen our presence in a warming Arctic."

Denmark is bolstering its security while resisting Chinese investments in Greenland, an autonomous Danish territory, including successfully pressuring the state-owned China Communications Construction Co. to withdraw its bid to build and manage Greenland's airports. Denmark is partially funding the projects.

Copenhagen will raise defense spending by $4.2 billion to improve security in Greenland, the Arctic and the North Atlantic. It also will add 16 U.S.-built F-35 fighter jets to its fleet of 43 to "significantly strengthen" the Danish Armed Forces, Defence Minister Troels Lund Poulsen stated.

Denmark will protect its strategically important maritime choke points. The country has contracted to buy coastal defense missile systems from Norway for more than $117 million, with first deliveries anticipated in 2026, Defense News magazine reported in December 2025.

Denmark, Finland, Iceland, Norway and Sweden comprise the Nordic Defence Cooperation (NORDEFCO) group to strengthen "national defense, explore common synergies and facilitate efficient common solutions." NORDEFCO's Vision 2025 plan calls for cooperation among the nations in peacetime, crisis or conflict, and especially to deter terror, cyber and hybrid threats.

"The Nordics work very, very well together," Dr. Adam Lajeunesse, an associate professor at Canada's St. Francis Xavier University whose research includes Arctic sovereignty and security, told FORUM. "They've got a single common view of what needs to be done and are moving in a fairly coordinated fashion."

Norway's 2025-2036 Defence Plan pledges increased

The U.S. Coast Guard icebreaker Storis prepares to moor in Seattle, Washington, in July 2025.
PETTY OFFICER 3RD CLASS ANNIKA HIRSCHLER/U.S. COAST GUARD

defense spending and asserts that "maintaining situational awareness in the High North and in the North Atlantic is paramount." The plan calls for increased maritime security capabilities, including acquiring at least five new frigates and five submarines, to protect Norway's more than 100,000 kilometers of mainland, island and fjord coastlines.

Oslo will buy satellites and long-range surveillance drones, and bolster air defenses with ground-based systems and other capabilities. The Norwegian Army will expand by two brigades, buy long-range precision fires and helicopters, and increase stocks of munitions, spare parts, fuel and equipment. "The rise of China is asserting pressure on the prevailing world order and an assertive Russia is challenging the Euro-Atlantic security architecture," the plan states.

Sweden also will raise defense spending. "We need to scale up production. We need to transform economic clout into combat power as well," Swedish Defence Minister Pål Jonson said while meeting with U.S. Secretary of War Pete Hegseth in Washington, D.C., in December 2025. Jonson said Sweden will provide security and deliver hard power to ensure it defends "every inch of allied territory."

Along with enhancing its icebreaker fleet, the U.S. will ensure a robust defense to counter Arctic threats, according to an October 2025 White House memorandum that addresses "growing strategic competition, aggressive military posturing, and economic encroachment by foreign adversaries." Among other military initiatives, the U.S. is enhancing training of personnel and allied forces for polar operations.

The North American Aerospace Defense Command (NORAD), a Canada-U.S. mutual defense entity, has intercepted Chinese and Russian military aircraft conducting exercises in Alaska's air defense identification zone.

Iceland, too, is shoring up security capabilities. Under a policy adopted in September 2025, Reykjavik will increase domestic preparedness and cooperation with multinational groups such as NORDEFCO. "Iceland's remote location, distance and isolation no longer suffice against external threats; they are, instead, creating specific challenges," the International Institute for Strategic Studies, a London-based think tank, reported in November 2025.

The Arctic's NATO countries are concerned about China's growing knowledge of undersea conditions, which could benefit submarine deployments, military experts say.

Royal Canadian Air Force CF-18 Hornets drill during the North American Aerospace Defense Command's Operation Noble Defender in March 2025.
SENIOR MASTER SGT. ANDREW SINCLAIR/U.S. AIR NATIONAL GUARD

"WE HAVE A TENDENCY TO TREAT THE CHINESE AS THOUGH THEY'RE A GREAT ARCTIC POWER. THEY'RE NOT."

~ **Dr. Adam Lajeunesse**, Canada's St. Francis Xavier University

CHINA'S ARCTIC AMBITIONS

Beijing's portrayal of its involvement in the Arctic as a win-win for itself and other states is becoming more difficult to accept as its relationship with the West sours and its ties with Russia grow, the Wilson Center, a U.S.-based research institute, reported in August 2024. Beijing and Moscow increasingly are linked in Arctic matters, especially since their leaders declared a "no-limits" strategic partnership days before the Kremlin's war against Ukraine began. But the authoritarian regimes have different outlooks: While Russia aims to divide other Arctic nations, China seeks to join and influence.

While China's actions in the Arctic warrant attention, Russia remains the most potentially troublesome actor, observers say. It's important not to overestimate Beijing's regional clout, Lajeunesse said. "We have a tendency to treat the Chinese as though they're a great Arctic power. They're not."

With many of its Arctic ambitions unfulfilled, China is focused on steadily building its capacity to operate in the region and using soft power, from economic investments to science diplomacy, to fashion itself as a legitimate stakeholder, the U.S.-based Rand Corp. research group reported in February 2025.

China's dual-use endeavors are obvious, Eiterjord, of The Arctic Institute, wrote in The Diplomat magazine in April 2025. Under the Chinese Communist Party's strategy of military-civil fusion, the shipyards that build the nation's cargo fleet also underpin its rapidly expanding navy, while many of the country's designers of research vessels also develop its warships.

Satellites, robotic arms and launch systems can serve commercial and military purposes, a U.S. congressional committee reported in November 2025. Unclear distinctions between China's state-owned enterprises and its nominally private firms add to the confusion.

Among 64 research and survey vessels deployed on Chinese oceanographic missions worldwide since 2020, more than 80% "demonstrated suspect behavior or possess organizational links suggesting their involvement in advancing Beijing's geopolitical agenda," the Center for Strategic and International Studies (CSIS), a U.S.-based policy research group, reported in 2024. Many of the ships operated in the South China Sea and the Western Pacific.

Beijing insists the China-Iceland Joint Arctic Science Observatory near Akureyri, Iceland, and the Yellow River Station, a research outpost in Svalbard, Norway, are purely scientific ventures, but the operations have raised speculation about ulterior motives, The Arctic Institute reported in October 2025.

Much of China's Arctic effort is aimed at developing the Northern Sea Route (NSR) atop Asia for international shipping and acquisition of oil, natural gas, minerals and fish. The undertaking entails collaboration with Russia, and both regimes benefit from an increasingly accessible channel. But Beijing and Moscow differ in their characterization of the Arctic and its maritime passages. While China has called the Arctic the "common heritage of humankind," Russia, with more than half of the Arctic coastline, takes a possessive stance, insisting it's the domain of Arctic states.

U.S. Secretary of War Pete Hegseth, left, and Swedish Defence Minister Pål Jonson meet in Washington, D.C., in December 2025.
PETTY OFFICER 1ST CLASS ERIC BRANN/U.S. NAVY

China provided Russia with a range of goods via the NSR in 2024, including chemicals, construction materials, automobiles and clothing, the U.S. congressional committee reported. Meanwhile, Russian exports to China via the NSR were mostly crude oil and liquefied natural gas, shipments that violate international sanctions against Moscow but help Russia find markets for its energy resources while providing China with inexpensive fuel.

The partnership between China and Russia, especially their military overflights and naval exercises on the polar region's fringes, concerns Arctic nations. "Strategic competition is one thing, but the flexing of military muscles is a major escalation in tension," The Arctic Institute reported. □

Road Map for Success

Philippine and United States Soldiers conduct a live-fire drill during Exercise Balikatan 2025 in the Philippines. REUTERS

U.S. ARMY PACIFIC'S OPERATION PATHWAYS
Nurtures Enduring Relationships

COL. DAVE BUTLER/U.S. ARMY PACIFIC

The United States Army Pacific's (USARPAC) Operation Pathways encompasses multinational exercises, rotational deployments and training engagements to maintain U.S. forces in a forward posture, ready to respond to an array of contingencies. Operation Pathways is a cornerstone in reinforcing alliances and enhancing interoperability with key regional partners. By training for humanitarian assistance and crisis scenarios, U.S. and partner forces build mutual trust and ensure seamless coordination during real-world missions.

Given the Indo-Pacific's unique geographic and geopolitical dynamics, partnerships are critical. Gen. Ronald Clark, commanding general of USARPAC, emphasizes that "partnerships matter, and you can't wait until crisis to make friends. It's too late." Operation Pathways is crucial to ensuring a free, secure and prosperous Indo-Pacific, helping partner nations build their capacity and capabilities. That includes developing joint interior lines, access, basing and overflight "so we have positional advantage in crisis or conflict [that] will allow us to deter our adversary, and should deterrence fail, be able to fight and win at a time and tempo of our choosing," Clark told the Foundation for Defense of Democracies, a U.S.-based think tank, in March 2025.

Pathways incorporates deliberate sequenced operations, activities and investments to rehearse rapid deployment of command and control, all-domain awareness, force protection, sustainment, and multidomain capabilities to key terrain. This strategic approach allows USARPAC to campaign and set the theater in ways that achieve positional advantage. Operation Pathways creates a consistent presence that demonstrates the U.S. Army's ability to overcome logistical challenges in one of the world's most complex operating environments.

As part of the operation's annual cycle, USARPAC Soldiers conduct more than 50 exercises with about two dozen countries, including the five U.S. treaty allies in the U.S. Pacific Command (US PACOM) area of responsibility: Australia, Japan, the Philippines, the Republic of Korea and Thailand. Multinational drills include Balikatan in the Philippines, Tamiok Strike in Papua New Guinea, Cobra Gold in Thailand, Super Garuda Shield in Indonesia, Yudh Abhyas in India, Keris Strike in Malaysia and Talisman Sabre in Australia.

The program also enables engagement with nations across Oceania and Southeast Asia. These partnerships are vital to address shared security concerns, build collective capacity and reinforce regional institutions that support long-term stability. By working with a broad range of Allies and Partners, the U.S. Army extends its influence beyond traditional defense relationships, creating a land power network built on trust and interoperability. The increasing scope, duration and multinational participation

in Operation Pathways exercises is a prominent trend emerging from changes in the strategic environment. Regionally and globally, countries are expanding their security contributions and focusing on cooperation, including territorial defense.

"Credible, prompt and sustained combat power, visible across the Indo-Pacific region, will deter acts of military aggression that destabilize the region, undermine security, and stability, and threaten the security, freedom, and prosperity of the United States," Adm. Samuel J. Paparo, Commander of US PACOM, told U.S. lawmakers in April 2025.

Enduring Presence

Operation Pathways began in 2014, when a U.S. Army unit exercised with counterparts from Indonesia, Japan and Malaysia. Formerly known as Pacific Pathways, the initiative united independent exercises into a single, cohesive operation to increase USARPAC's regional presence and cut transportation costs. The program has expanded to include thousands of personnel from a growing roster of partner forces.

Now known as Operation Pathways 3.0, the program has significantly grown since 2014. U.S. Army I Corps increasingly integrates National Guard and Reserve units to leverage their skills and experience in training with partner nations. Forces rehearse strategic movement, operational maneuver and tactical employment of land forces at size and scale throughout the region's diverse terrain and over extended distances.

Critically, the program's enduring regional presence — a key refinement over the years — has nurtured increasing commitment among partners, including investments of time and resources.

Operation Pathways task forces typically are deployed to host nations and regions for 90 days. The extended

Gen. Ronald Clark, left, commander of U.S. Army Pacific, and Gen. Maruli Simanjuntak, chief of staff of the Indonesian Army, exchange gifts during the 2025 Land Forces Pacific Symposium in Honolulu, Hawaii. STAFF SGT. CAROLINA SIERRA/U.S. ARMY

U.S. Soldiers conduct sling load operations training in March 2026 in preparation for Operation Pathways 2026.
SGT. AUSTIN PAREDES/U.S. ARMY

training is essential to facilitate learning at an elevated level, according to Dr. Michael Krivdo, USARPAC historian. Participants learn about cultural relationships among countries while fostering rapport at the individual and organizational levels. Units maintain those relationships after returning home, Krivdo said.

The sustained presence also enhances the collection of information critical to understanding the operational environment.

"Multilateral trainings paint a picture of shared vision and unity of purpose among participating states to produce an integrated deterrent effect," Gen. Romeo Brawner Jr., then chief of staff of the Armed Forces of the Philippines, said during the Land Forces Pacific Symposium in Hawaii in 2023. "By training together, we are building each of our own capabilities and really building on that interoperability so that, if the need arises, we would be able to work together. The objective is to deter war. Making sure that the world knows that we are working together, we could keep that lethal punch unnecessary."

Operation Pathways fundamentally is about building trust and long-term relationships. "These partnerships are not built overnight; they are forged through years of collaboration, mutual respect, and a shared vision for a Free and Open Indo-Pacific," U.S. Army Maj. Gen. James Bartholomees, commander of the 25th Infantry Division, said during the Yama Sakura exercise with Australian and Japanese forces in Japan in August 2025. Extended deployments in the region demonstrate that the U.S.'s commitment is not merely a fly-in, fly-out approach. Moreover, they allow the U.S. to support partners in building their capabilities and capacity.

"It is about building trust, fostering mutual understanding, and enhancing interoperability across human, procedural, and technical domains," Bartholomees said. □

FORUM ILLUSTRATION

CODE SECURITY

A Singapore hub leads regional efforts to develop digital resilience

YEO SEOW PENG/ASSOCIATION OF SOUTHEAST ASIAN NATIONS DEFENCE MINISTERS' MEETING CYBERSECURITY AND INFORMATION CENTRE OF EXCELLENCE

The digital revolution has transformed Southeast Asia over the past two decades and delivered unprecedented economic opportunities. The region's digital economy, projected to reach $1 trillion by 2030, demonstrates how advancement in technology and connectivity boosts its economies. With more than 560 million internet users and digital penetration rates averaging 78.2% across the region (excluding Laos, Myanmar and Timor-Leste), the 11-member Association of Southeast Asian Nations (ASEAN) is riding this wave. Indonesia, for example, has 212 million internet users, ranking fifth worldwide, and Singapore has 96% internet adoption.

Running in tandem with rapid digital expansion, however, is an increase in threats in the cyber and information domains. The cost of cybercrime was estimated at $9 trillion globally in 2024, with ASEAN members experiencing a huge increase in cyberattacks compared to counterparts worldwide. East and Southeast Asian countries have lost up to $37 billion to cyber-enabled fraud in recent years.

Traditional and social media, meanwhile, remain the region's primary sources of information, with social media platforms gaining prominence as hubs for communication, entertainment and commerce. As elsewhere, a preference for information that conforms to existing beliefs at the personal and community levels leaves Southeast Asian societies vulnerable to misinformation and disinformation, especially around sensitive and emotive topics, including national security. With high rates of social media penetration in the region, misinformation and disinformation can be created and exchanged at unprecedented scale and speed, often outpacing verification or fact-checking efforts.

Compounding this challenge are significant disparities in digital literacy across age groups, geographical locations and socioeconomic strata. This creates fertile ground for exploitation by malicious actors seeking to manipulate public opinion or destabilize societies. The World Economic Forum's Global Risks Report 2025 identified misinformation and disinformation as the top global risk in the short term (defined as a two-year outlook) and ranked it fifth among long-term risks (10-year outlook). The report noted that technological advancement has dramatically amplified these threats. Fake accounts, divisive narratives and coordinated bot networks operate alongside sophisticated synthetic media, creating information pollution that can undermine institutional trust. The advent of generative artificial intelligence has further reduced the cost and complexity of creating disinformation, enabling even relatively unsophisticated actors to launch campaigns to manipulate public opinion and fracture societal cohesion.

Lt. Gen. Susan Coyle, the Australian Defence Force's then- joint capabilities chief, gives the keynote address at the third annual Digital Defence Symposium in Singapore in July 2025.
SINGAPORE DEFENCE MINISTRY

CONFRONTING DIGITAL THREATS

For the region's armed forces, developments in the digital space represent a fundamental shift in operational reality. The battlefield no longer is confined to, or defined by, physical terrain. Information warfare can complement or precede kinetic operations. Occurring in the gray zone, such slow-drip operations can appear innocuous at first and be difficult to detect.

Information campaigns also have emerged as strategic tools to create confusion during military operations. This has been evident in recent conflicts stretching from Europe to the Middle East and South Asia, with such tactics deployed across online platforms to influence domestic and foreign opinion.

Protecting against digital threats requires a whole-of-government approach incorporating the military, homeland security and other public entities, as well as the private sector. Multilateral and regional cooperation is crucial to effectively defend against evolving threats.

Defense establishments across Southeast Asia, however, are not yet fully structured to address information domain challenges. Some militaries view such issues primarily through a cybersecurity lens, focusing on the cyber domain as the main vector for misinformation and disinformation due to rampant online crimes and scams. Additionally, responsibility for tackling information threats typically falls under national communications or information ministries rather than defense establishments, creating coordination challenges when military operations intersect with information warfare. This highlights the complex nexus between information and cybersecurity, as well as the comprehensive approach required to address digital challenges.

ESTABLISHMENT OF ACICE

Digital domain threats were amplified during the COVID-19 pandemic when many services moved online. Since then, the scale and sophistication of threats have grown considerably, threatening critical infrastructure and networks, as well as potentially fracturing social cohesion within and across states. As such, during the ASEAN Defence Ministers' Meeting (ADMM) in 2021, leaders approved Singapore's proposal to establish the ADMM Cybersecurity and Information Centre of Excellence (ACICE). The decision reflected the defense sector's appreciation of the evolving landscape and the importance of leadership, initiative and foresight in addressing such threats.

ACICE embraces a dual approach. It promotes information sharing among militaries and other defense establishments regarding fake news, misinformation and disinformation, and cybersecurity threats. The center also builds regional capacity in dealing with cyber and information threats through exchanges and other cooperation, boosting trust and confidence.

The ACICE Malware Information Sharing Platform enables real-time dissemination of cyber threat intelligence, malware indicators of compromise, and common vulnerabilities and exposures among ASEAN militaries. The platform leverages ASEAN's collective knowledge to provide defense establishments with early warning, thereby facilitating timely mitigation of cyberattacks.

The Critical Infrastructure Defence Exercise in Singapore in late 2024 drew more than 200 participants from military, cybersecurity and other agencies. SINGAPORE DEFENCE MINISTRY

ACICE maintains a messaging app with daily and weekly updates on the cyber and information domains. The center has produced more than 130 analytical reports covering developments and trends, providing tactical insights into evolving techniques used by malicious actors. The reports provide situational awareness of emerging threats and analysis of case studies. By promoting information sharing, ACICE supports ASEAN members in developing fit-for-purpose defenses and mitigation measures.

BUILDING REGIONAL CAPACITY

ACICE focuses on practical cooperation by strengthening ASEAN's capabilities to address cyber and information threats through three main aspects:

- A panel of experts provides insights into trends and developments, bringing together academics, specialists and industry representatives to analyze challenges and share best practices.
- Seminars and dialogues facilitate the exchange of perspectives and expertise. ACICE's flagship event, the annual Digital Defence Symposium, includes senior defense and military officials, academics, and industry experts. The platform is the first of its kind in the region. The 2025 iteration attracted more than 300 participants from 30 countries, including Germany, Japan, the United Kingdom and the United States.
- Training courses and simulated exercises address how technology is transforming the information landscape. They prepare participants to recognize and assess disinformation threats and their potential impact on military operations, and to develop communication strategies for countering disinformation campaigns.

Leaders gather for the Association of Southeast Asian Nations Defence Ministers' Meeting in Kuala Lumpur, Malaysia, in October 2025. AFP/GETTY IMAGES

ACICE represents a milestone in ASEAN's approach addressing the complex challenges of the digital age. As cyber and information threats evolve and transcend national boundaries, the center serves as an inclusive platform for cooperation. While ACICE is anchored within ASEAN, its outlook extends beyond regional boundaries, leveraging a network of partners to further enhance the capacity of ASEAN militaries to deal with digital threats. The approach reflects the understanding that regional security in the digital domain requires internal cohesion and external partnerships. The region will only be stronger and more resilient if we can draw on the collective expertise and experience of our partners. □

FIGHTING DISRUPTION, DESTABILIZATION

FORUM ILLUSTRATION

How Indo-Pacific Nations Refute Manipulated Information

FORUM STAFF

Manipulated information campaigns threaten security by exploiting communication systems to undermine trust in social, political and strategic domains. False narratives in Myanmar, for example, included hate speech insisting Muslim minority Rohingya communities didn't belong in the country and accusations they were burning their own villages amid a 2017 government crackdown on insurgent groups. The social media-stoked violence left at least 6,700 men, women and children dead within a month, according to the medical charity Doctors Without Borders. Some of the nearly 700,000 people who fled to neighboring Bangladesh said mobs had joined Myanmar troops to attack and kill civilians, the BBC reported in 2020.

A 2018 Facebook video that falsely accused a Muslim restaurateur in Sri Lanka of spiking customers' food with "sterilization pills" — which don't exist — fueled ethnic violence, The New York Times newspaper reported. For days, mobs burned mosques, Muslim-owned shops and homes, killing at least one man and prompting a nationwide state of emergency.

In authoritarian nations, where regimes police news and social media reports, and censor information that contradicts official views, state-endorsed platforms do not simply publish news. They create a reality independent of verifiable facts. And "a core principle of a healthy democracy is having a common set of facts — a set of facts that we share and agree on," wrote Marites Dañguilan Vitug, editor of the Philippines-based Rappler news website. "Otherwise, we would be fragmented. We will not be able to have a conversation because our starting points diverge."

Information manipulation can disrupt and destabilize security, divide populations, and paralyze international relations. Artificial intelligence (AI) and other advances help weaponize information by increasing its scale, speed and sophistication, making it difficult to detect falsehoods and misleading content. ChatGPT maker OpenAI, for instance, said propagandists in China used the technology to mass-produce social media posts in multiple languages — and to generate comments that falsely imply the posts are receiving engagement that helps spread the distorted information to more social media users.

AI can also rapidly produce deepfakes, false but realistic video and audio clips that malign influencers use to twist the truth. During Taiwan's 2024 presidential election, China digitally generated fake news anchors to broadcast Beijing's preferred message. The goal was to influence

A voter casts a ballot in Taiwan's 2024 presidential election. Beijing repeatedly targets Taiwan's elections with manipulated information campaigns, analysts say.
KYODO VIA REUTERS

Taiwan residents attend a presidential election rally in 2024.
YOMIURI SHIMBUN VIA REUTERS

audiences on the self-governed island. Beijing also appeared to build an AI deepfake that altered a former Taiwan presidential candidate's voice, making it seem as though he was endorsing China's choice for office, The Wall Street Journal newspaper reported.

Beijing's efforts to interfere with the election failed, with Taipei emphasizing election transparency and proactive messaging to counter such tactics. Globally, however, information manipulation continues to be deployed as a cognitive warfare tactic to warp narratives around territory and sovereignty, fracture social cohesion within democracies, and cast doubt on international alliances that uphold stability. In answer, like-minded countries are strengthening resilience and developing robust responses to the evolving threat.

Taipei's resistance

Taiwan has earned its reputation for resilience by standing up to malign information campaigns. Its whole-of-society approach encompasses government vigilance, independent fact-checking groups, civic activism and public education.

Officials embrace a strategy of rapid response, learning to identify and discredit malicious messaging as quickly as possible. "Find it early, like a tumor or cancer," Alexander Tah-Ray Yui, Taiwan's economic and cultural representative to the United States, told The Associated Press (AP). "Cut it before it spreads." Taipei used the approach during the COVID-19 pandemic, holding daily briefings to quickly provide accurate information so rumors had less time to spread.

Independent networks screen online content, debunk fake claims and share verified information. Many of the organizations were established by ordinary citizens, such as MyGoPen founder Charles Yeh, who created the fact-checking chatbot service after realizing that online rumors were confusing his relatives, the AP reported. Others, including the Taiwan FactCheck Center, say they preserve their independence in part by declining government funding. When manipulated video accused officials of fraud during the 2024 election, popular YouTube broadcasters published videos explaining how Taiwan's vote-counting system works.

Media literacy — the ability to access, analyze and evaluate content — is part of Taipei's school curriculum. Organizations such as Fake News Cleaner host workshops and outreach events to educate residents — from children to seniors — on combating information manipulation. Fact-checkers publicize the methods that malign actors use, essentially "prebunking" before dangerous narratives take hold. Social scientists refer to the tactic as inoculation against disinformation.

Taipei uses AI detection tools to spot deepfakes and other deceitful means of spreading harmful narratives. Cyber Ambassador Audrey Tang said it is "crucial that AI is trained to serve the greater good, while unlocking our collective wisdom and building a more accountable and participatory digital society." Transparency is the way forward, she said during the June 2025 launch of the Artificial Intelligence Advisory Group on Elections in Washington, D.C., calling for civil society and government to "co-govern" the technology.

"Taiwan has become a sought-after voice in global AI governance," The Diplomat magazine reported. "In effect, it has already lived the future others fear, emerging stronger on the other side of AI-fueled disinformation by harnessing the technology's potential."

France fights back

France is countering foreign malign information while seeking to safeguard democratic principles such as free expression. Paris prioritizes legislation crafted to manage risks without introducing government censorship.

Policymakers contend that manipulated information, particularly when created and disseminated by foreign actors, threatens security, social cohesion and election integrity. Paris opted for a legal response after 2017, when Russia aimed its malign information machinery at France's presidential election. Days before the final voting, hackers published information — including emails and forgeries — purportedly from candidate Emmanuel Macron's campaign. The influence attempt failed to significantly affect results — Macron was elected to his first term — but succeeded in raising French awareness and determination to fight back. Because of the nation's long constitutional tradition of free speech, lawmakers crafted legislation that criminalizes the spread of false or manipulative information aimed at misleading the public, but the 2018 law does not target opinions.

It empowers judges during election periods to order the removal of "inaccurate or misleading allegations or statements likely to affect the sincerity of the vote" when they are "disseminated on a massive scale in a deliberate, artificial or automated manner via an online public communication service." The legislation also requires digital platforms to disclose the sponsors of paid content.

France leverages the open-source Disinformation Analysis and Risk Management (DISARM) framework to detect, scrutinize and mitigate manipulated information. Drawing on global best practices, the framework emphasizes sharing data and analysis to counter malign information. The DISARM Foundation also maintains a database of influence operations, providing a common language for sharing intelligence and understanding manipulative behavior. Analysts say the mechanism enables authorities to respond to false and misleading information

case by case instead of using blanket restrictions.

France's Service for Vigilance and Protection against Foreign Digital Interference (Viginum), meanwhile, focuses on countering foreign information manipulation and interference. To ensure the agency would not be used to censor opposition or restrict free speech, Paris created criteria to distinguish domestic from foreign information. "Its focus was solely on massive, purposeful, artificial, or automated dissemination of manifestly inaccurate or misleading content," Dr. Agnieszka K. Cianciara, an associate professor at the Polish Academy of Sciences, wrote for the EU-Values Network. "An independent Ethical and Scientific Committee provided oversight." Viginum identifies and exposes threats. It does not remove online content but provides evidence that can trigger legal processes, diplomatic responses or public warnings.

France's layered approach is designed to balance security and free speech. Citizens can express controversial opinions. When foreign malign actors embark on clandestine influence campaigns, however, government can intervene. Using the DISARM system to assess risk and Viginum to pull back the curtain on foreign interference, France does not broadly criminalize falsehoods or allow the government to define truth. Instead, it targets coordinated campaigns that aim to distort democratic debate.

Manila exposes aggression

As the Philippines confronts Beijing's aggression in the South China Sea, it also must battle skewed narratives about maritime rights in the region. One of its weapons is "The Stories of Teacher Jun," a 40-page comic book unveiled in early 2025.

Public education and outreach help the archipelago's 118 million citizens understand and counter malign influence campaigns. Beijing illegally claims almost all of the South China Sea, asserting "historic" rights to territory inside the Philippines' exclusive economic zone (EEZ), where international law gives a country sole rights to resources. With the comic, Philippine national security leaders explain Manila's legal rights in the sea and the 2016 international tribunal ruling that invalidated China's claims, simplifying complex maritime law and sovereignty issues with accessible language.

"Teacher Jun" complements official transparency and civic fact-checking as part of the Philippine strategy to defeat malign messaging. Manila also uses photographs,

The comic book, "The Stories of Teacher Jun," explains the Philippines' rights in the South China Sea. REUTERS

ABOVE: A China Coast Guard ship is seen through binoculars from the Philippines' Thitu Island. THE ASSOCIATED PRESS

A China Coast Guard vessel fires a water cannon at a Philippine craft in the South China Sea in December 2024. NATIONAL TASK FORCE – WEST PHILIPPINE SEA

videos and other evidence to expose Beijing's aggression in the South China Sea. Since 2023, Philippine officials have documented and publicized dangerous actions by China Coast Guard, navy and maritime militia vessels. Chinese personnel fire water cannons at smaller Philippine vessels, block patrols and fishing crews, pursue and ram Manila's ships and, in one instance, used knives and other weapons to threaten and injure Philippine military personnel.

While China has used such tactics for years, it often happened outside public view, allowing Beijing to deny allegations. By exposing the antagonism, the Philippines rallied domestic and international support and refuted Beijing's claim that it is not an aggressor. Meanwhile, civil society has joined the fight. One such organization, Atin Ito! (This is Ours!), has led humanitarian missions to support fishing crews in the Philippines' EEZ. The resulting international news coverage infuriated Beijing, which released social media content falsely claiming the group is funded by the Philippine and U.S. governments.

Philippine lawmakers and other officials consider foreign malign influence a national security threat. Senate hearings and a presidential probe into foreign election interference increased scrutiny on the sources of inauthentic content and signaled a willingness to investigate potentially foreign state-backed campaigns. Such inquiries deter covert influence operations and generate public records to contest false claims.

"The challenge for the Philippine government is to invest resources to study disinformation from China, including those from local proxies," wrote Vitug, the Rappler editor. "It must work with experts not only from the Philippines but from friendly countries like Canada, Australia and the United States, to track down sources of false news, patterns and trends, conduct digital forensic investigation and build national digital literacy. This will enable the Philippines to come up with a more effective, data-driven response, backed by scientific information." □

ACQUIRING DEEP SKILL

PMTEC Pushes Asymmetric Advantage

TAI PROHASKA/UNITED STATES PACIFIC MULTI-DOMAIN TRAINING AND EXPERIMENTATION CAPABILITY

In the Indo-Pacific, where distance and dynamic threats demand unparalleled readiness, the United States' Pacific Multi-Domain Training and Experimentation Capability (PMTEC) empowers warfighters to cultivate mastery through realistic, multidomain training environments.

Established in 2022, PMTEC is funded and resourced by the U.S. Pacific Command (US PACOM) to enhance joint, combined and coalition warfighting readiness, posture and lethality. Through repetition and exposure to evolving scenarios integrating live, virtual and constructive (LVC) training, the PMTEC team ensures warfighters build the muscle memory needed to quickly and effectively respond in highly complex situations to provide sustainable asymmetric advantages to U.S., ally and partner forces.

The 2025 U.S. National Security Strategy (NSS) frames the Indo-Pacific as "among the next century's key economic and geopolitical battlegrounds," requiring technological superiority, sustained deterrence and coalition strength. PMTEC flexes asymmetric advantage in all three pillars, as well as interoperability among the U.S. joint forces and with Allies and Partners.

As a key component of the Pacific Deterrence Initiative, PMTEC reinforces the U.S. commitment to homeland defense and a free, secure and prosperous Indo-Pacific. PMTEC's integration of advanced training technologies and its alignment with the NSS make it a cornerstone in maintaining regional stability and countering aggression.

The United States' Pacific Multi-Domain Training and Experimentation Capability (PMTEC) enabled integration of the Joint Deployable Electronic Warfare Range during Exercise Balikatan 2025 in the Philippines to simulate realistic enemy air defense threats for pilot training.

SGT. MITCHELL JOHNSON/U.S. MARINE CORPS

Realistic Threat Scenarios

LVC training environments allow warfighters to rehearse against simulated adversaries that mirror real-world threats across land, sea, air, space and cyber domains, ensuring comprehensive readiness. For example, during Exercise Balikatan 2026 in the Philippines, PMTEC supported the integration of emitters that simulate the electronic signature of an enemy force, providing a signal for the Canadian,

U.S. Marines fire an M224 81 mm mortar during the annual Fuji Viper exercise at Camp Fuji, Japan, in December 2025.
CPL. BRISEIDA VILLASENOR/ U.S. MARINE CORPS

Japanese, Philippine and U.S. combined task force's electronic warfare (EW) specialists to hunt. Next-generation command and control relies on EW capabilities to validate and shoot targets, said U.S. Army Capt. Phoebe Lee, artillery fire control officer, 25th Infantry Division. "Everything you saw leave [during a Balikatan 2026 counter-landing exercise] was a full digital kill chain," she said. "Those targets were being sent completely digitally to the Fire Direction Center. We keep pushing forward with it [EW], and we're getting better and more lethal."

Other technologies being integrated into training include artificial intelligence (AI), tactical assault kits (TAK) and deployable cyber ranges (DCR). These tools give warfighters real-time insights, situational awareness and seamless communication, enabling faster and more informed decisions.

"By integrating AI and TAK devices into training environments, PMTEC ensures that warfighters are exposed to realistic scenarios with AI-enabled tools that challenge their decision-making and operational skills," said Mary Ann Swendsen, PMTEC experimentation integrator. "This level of threat-informed realism is critical for developing innovative ways and AI-assisted efficiencies that lead to operational superiority."

DCRs provide realistic training against cyber threats in a joint force and coalition environment. PMTEC supported the DCR for Super Garuda Shield 2025 in Indonesia. The exercise combined forces from 23 nations, reinforcing distributed operations and coalition deterrence. The DCR was pivotal in enhancing threat awareness, joint force readiness and interoperability for cyber defense.

Indonesian National Armed Forces 2nd Lt. Vian Navalilno was a team leader during the cyber exercise. He said the simulated threats and working side by side with U.S. and coalition forces greatly increased his capabilities and confidence. "It was totally realistic, based on real-world scenarios," Navalilno said. "It was my opportunity to identify the latest techniques, tactics and procedures." He said the lessons will help him identify real-world threats, share information with

Allies and Partners, and work collectively to prevent and respond to cyberattacks.

Realistic cybersecurity training with Allies and Partners also is critical to homeland defense. The 2025 Homeland Threat Assessment emphasized that cyber threats are among the most pressing dangers to the U.S., cutting across mission areas such as public safety, border security, infrastructure and economic stability.

"Cyberattacks aren't just about stolen data," Swendsen said. "They're about strategic positioning. Adversaries weaponize data to weaken deterrence, facilitate confusion, shape narratives and prepare the battlefield without firing a shot."

Sustained Deterrence

To prepare for combat, warfighters need realistic training that sharpens their tactical skills under stress and builds unit cohesion in ways that simulations alone cannot achieve. To that end, PMTEC enhances joint experimentation with new concepts, including multidomain targeting and battle management.

Sling Stone 2024, a US PACOM-led capabilities exercise that coincided with the Missile Defense Agency's (MDA) Flight Experiment Mission-02 in the U.S. territory of Guam, showcased PMTEC's ability to integrate virtual and constructive simulations with live forces. That enables joint and coalition forces to rehearse sensitive tactics, techniques and procedures without being exposed to adversaries.

"Sling Stone was able to rapidly transition from a virtual event using distributed training systems based in the U.S. and live units on Guam to a bilateral U.S.-Japan defense of Guam scenario," said U.S. Navy Cmdr. Ben Herring, then assistant to the MDA director at US PACOM.

The first phase included LVC training environments simulating real-world multidomain operations in the air and on land and sea. The second phase used the MDA's test of a missile defense interceptor to allow the joint force to detect, track and simulate engagement of the threat. During the test, a Standard Missile-3 Block IIA, fired from a vertical launcher at Andersen Air Force Base, Guam, intercepted a surrogate medium-range ballistic missile more than 200 nautical miles off the coast of northeast Guam.

Simultaneously, the U.S. Navy guided-missile destroyer USS Milius, operating off Guam, detected, tracked and simulated engagement of the missile. Task Force Talon, the U.S. Army's Guam-based Terminal High Altitude Area Defense unit, also received missile tracking information.

The Japan Maritime Self-Defense Force guided-missile destroyer JS Haguro also exercised its air defense support, increasing interoperability between forces and fostering a shared information environment.

"Leveraging MDA's flight test to train how we fight just made sense," said U.S. Navy Rear Adm. Greg Huffman. "We will take lessons learned and continue to strengthen the architecture of Guam's defense against evolving adversary missile threats."

Enabling Interoperability

While live-fire exercises span the gap between classroom theory and battlefield reality, PMTEC builds additional bridges — nodes, networks and facilities — that link geographically distributed ranges across the Indo-Pacific and beyond with U.S. continental assets. Connecting live ranges with virtual simulators and constructive (computer-generated) environments enables realistic training without revealing sensitive tactics to adversaries — another asymmetric advantage.

Indonesian and U.S. Soldiers conduct a PMTEC-supported cyber exercise during Super Garuda Shield 2025 in Indonesia.

SGT. SEAN WALKER/U.S. ARMY NATIONAL GUARD

WHAT IS LIVE, VIRTUAL AND CONSTRUCTIVE TRAINING?

LIVE — Real-world operations with personnel, equipment and platforms. It provides hands-on experience in field exercises, live-fire drills and other environments.

VIRTUAL — Computer-based simulations that replicate real-world scenarios. Participants interact with simulated environments through virtual reality and other technologies.

CONSTRUCTIVE — Computer-generated forces and scenarios that simulate operational environments. This enables large-scale complex training that may not be possible to replicate in live environments.

A Standard Missile-3 Block IIA is fired from Andersen Air Force Base, Guam, as part of the U.S. Missile Defense Agency's Flight Experiment Mission-02 in late 2024.

NANCY JONES-BONBREST/
U.S. MISSILE DEFENSE AGENCY

PMTEC has created a unified training ecosystem capable of integrating simulation systems across locations, ensuring combined joint forces can train together effectively, regardless of physical barriers.

"PMTEC has established the largest coalition range system in the world," said Dr. Andre J. Stridiron III, PMTEC program manager.

Enabling the U.S. and its Allies and Partners to rehearse joint operations in a unified training environment with realistic scenarios tailored to regional threats is a significant asymmetric advantage for the U.S. and coalition forces.

Balikatan 2026 marked a significant milestone for coalition command and control in the Indo-Pacific, as allied forces for the first time had a common operating picture accessible to eight nations, enabled by PMTEC. Alphonse La Porta, a career diplomat and former U.S. ambassador to Mongolia, served as political and military advisor for the exercise's control group. He said contextual awareness and information flow are invaluable for commanders. "We can't go to war without effective command and control," La Porta said. "We have to make doggone sure that it works."

Near-peer adversaries may have large militaries but often lack true allies. Their partnerships are transactional, fragile and limited. By contrast, U.S.-led coalitions are built on shared values, trust and institutional frameworks, giving them staying power and credibility. That imbalance makes coalitions an asymmetric advantage. Unlike raw military strength, coalitions bring unique benefits that tilt the balance strategically, psychologically and operationally.

During large-scale military exercises such as Cobra Gold 2026 in Thailand, the use of TAK devices and a common operating picture allows warfighters to overcome language barriers and other procedural differences, enhancing interoperability and strengthening partnerships.

By demonstrating a synchronized, technologically advanced, and highly interoperable network of Allies and Partners, asymmetric advantage serves as a powerful deterrent. It reduces the likelihood of miscalculation and escalation by showcasing the readiness and capability of U.S. and allied forces to respond decisively to any threat.

PMTEC's ability to rehearse tomorrow's fight with Allies and Partners without revealing tactics or risking escalation is a strategic asset in maintaining stability in the Indo-Pacific.

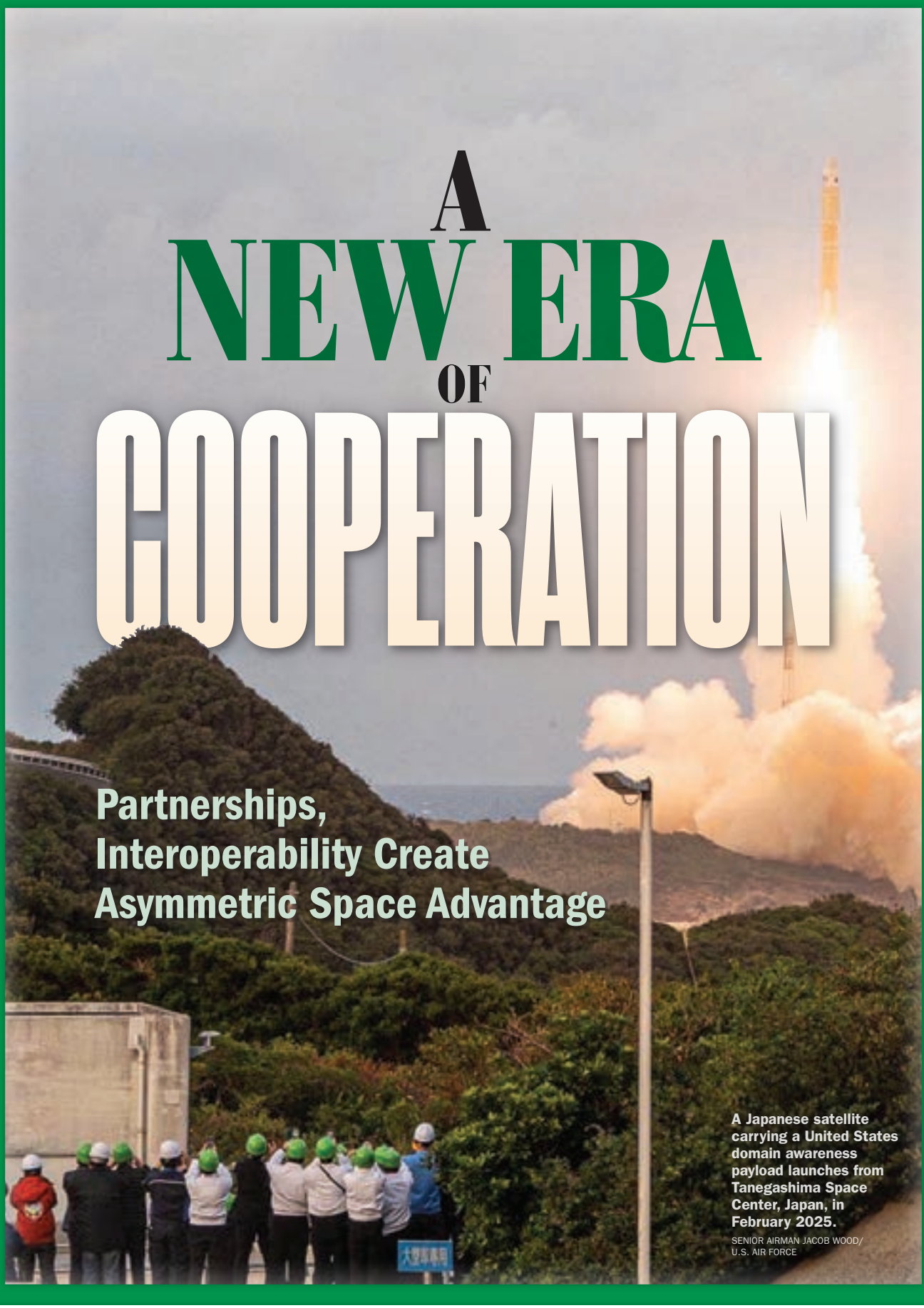
PMTEC exemplifies the principle of "going deep," empowering warfighters to go beyond surface-level preparation and cultivate the practiced expertise required to excel in complex, multidomain, contested scenarios. This unwavering commitment to depth — in skill, strategy, resources and collaboration — ensures that U.S. and coalition forces are not only prepared to meet today's challenges, but also well-equipped to adapt and prevail in the face of tomorrow's uncertainties. PMTEC is diving deep to keep U.S. asymmetric advantage clearly visible on the surface, projecting strength and readiness across the Indo-Pacific and beyond.

"We are continuously … integrating emerging technologies, creating infrastructure and partnering with industry to operationalize exercises and enhancing U.S. posture and deterrence," Stridiron said. "We are bringing kinetic and nonkinetic — cyber, electronic warfare, space, information — together to create realistic, real-time, multidomain training with our coalition partners." □

Tai Prohaska is an information operations integrator supporting the Pacific Multi-Domain Training and Experimentation Capability.

A NEW ERA OF COOPERATION

Partnerships, Interoperability Create Asymmetric Space Advantage



A Japanese satellite carrying a United States domain awareness payload launches from Tanegashima Space Center, Japan, in February 2025.

SENIOR AIRMAN JACOB WOOD/ U.S. AIR FORCE

FORUM STAFF

In an increasingly contested orbital environment, the United States Space Force is augmenting its approach to space security and defense cooperation. With the release of its 2025 International Partnership Strategy, in support of U.S. Department of War (DOW) objectives, the Space Force has built a strategic vision on collaboration, interoperability and shared responsibility among the U.S. and its Allies and Partners. The approach aligns with the U.S. National Defense Strategy and the DOW International Space Cooperation Strategy.

Space defenders from Australia, the Republic of Korea, Singapore and the U.S. participate in exercise Cobra Gold 2025 in Thailand.

TECH. SGT. EMERSON NUÑEZ/U.S. SPACE FORCE

"Space power is the ultimate team sport," Gen. B. Chance Saltzman, then U.S. Space Force Chief of Space Operations stated in July 2025. "Space is simply too complex, too vast and too risky for any single power to control. Therefore, if the service is to achieve its mission to secure our nation's interests in, from and to space, then it absolutely must cultivate partnerships with partners upon whom it can depend on to share its pursuit of a stable, secure and sustainable domain."

Space has evolved from a realm of scientific exploration to a strategic domain central to national security. It supports essential functions including global communications, navigation, missile defense systems, Earth observation and battlespace intelligence. Threats from anti-satellite weapons, maneuverable spacecraft and other capabilities are increasing, especially from authoritarian regimes, which pursue capabilities that could interfere with or damage vital satellites.

Military and civilian actors recognize the necessity of shared approaches to space security, specifically robust partnerships that enhance deterrence, resilience and responsible spacefaring behavior.

Strategic Imperative

The defining theme of the Space Force's strategy is interoperability — with systems, data and personnel from different nations operating seamlessly. The International Partnership Strategy includes three goals to maintain space superiority and deter conflict:

- ***Empowering Allies and Partners*** to be force multipliers to secure collective interests.
- ***Enhancing communication*** by ensuring interoperable data, capabilities and activities while maximizing information sharing across classification levels.
- ***Integrating partners*** across force design, development and employment.

The objectives require common standards for data, communication and operational concepts on a military and strategic level. The result will be allied and partner forces that can share information and respond jointly during crises.

Such interoperability is not a new concept. For decades, entities including NATO and the intelligence-sharing group among Australia, Canada, New Zealand, the United Kingdom and the U.S. have emphasized shared technical and procedural standards. Space, however, presents unique challenges. The speed of operations, lethality of threats and dual-use nature of many assets make real-time interoperability critical.

The Space Force's holistic international strategy identifies lines of effort that span from the earliest stages of capability planning to joint operations, signaling the significance of partnership to space security objectives:

- ***Creating conditions*** to integrate Allies and Partners' military personnel into the Space Force.
- ***Involving Allies and Partners*** in force development, which includes identifying and allocating resources.
- ***Operating seamlessly*** as a coalition in exercises and real-world operations.

Members of the Japan Air Self-Defense Force Space Operations Group and U.S. Space Force Guardians celebrate the first anniversary of U.S. Space Forces-Japan in November 2025.
DAVID DOZORETZ/U.S. SPACE FORCE

"So you can see that touches every single part of the Space Force," U.K. Royal Air Force Air Marshal Paul Godfrey said at the 2025 Space Symposium in Colorado. Godfrey, in an exchange role with the U.S. Space Force, led the partnership strategy's development and told Air & Space Magazine he is particularly interested in interoperability. He said different data links hampered cooperation when he was a fighter pilot in the 1990s.

Saltzman and other senior leaders emphasize that interoperability is not only conceptual but also operational, with shared data standards and planning, integrated training, and joint exercises. Interoperability could mean Allies and Partners sharing real-time space domain awareness, participating in combined satellite maneuvers, operating under shared doctrines for crisis response and conducting combined missions under established procedures.

Cornerstone of Cooperation

One example of multinational cooperation is the Combined Space Operations (CSpO) Initiative. Founded in 2014 with four nations, it now includes 10 spacefaring nations: Australia, Canada, France, Germany, Italy, Japan, New Zealand, Norway, the U.K. and the U.S. The program advances goals similar to the U.S. Space Force's international strategy, promoting cooperation, interoperability and resilience, and intelligence sharing. Its vision underscores the shared commitment to collective security and sustainable use of space, guided by principles such as freedom of use and adherence to international law.

In late 2025, leaders from CSpO nations met in Toulouse, France, to reaffirm their commitment to interoperability and space security capabilities. U.S. Space Force and U.S. Space Command (USSPACECOM) officials stressed that integrated coalition capabilities

Gen. Stephen N. Whiting, left, commander of the U.S. Space Command (USSPACECOM), and Air Vice-Marshal Darryn Webb, chief of the Royal New Zealand Air Force, sign an agreement to place a New Zealand liaison officer with USSPACECOM.
CHRIS DEWITT/U.S. SPACE FORCE

Then-U.S. Space Force Chief of Space Operations Gen. B. Chance Saltzman speaks during the Air and Space Power Conference in Canberra, Australia, in May 2024. AUSTRALIAN DEFENCE DEPARTMENT

Republic of Korea and U.S. officials stand in front of the Combined Joint Space Operations Center at Osan Air Base, South Korea, in March 2025. 2ND LT. JIMMY NGUYEN/U.S. AIR FORCE

are essential to counter rapidly advancing threats. Gen. Stephen N. Whiting, commander of USSPACECOM, emphasized the "jaw-dropping speed" at which competitors are advancing in space, requiring "integrated coalition capabilities that deter aggression" and defend Allies and Partners' interests.

"We are building a coalition capable of addressing the challenges of a contested space environment," Saltzman said at the gathering. "To be effective, we must collaborate on our architectures, integrate our training, exercises and operations, and build a common understanding of the threats we face."

Such CSpO cooperation dovetails with the Space Force's interoperability goals, broadening the coalition of nations that train, plan and operate together in a crowded domain.

Regional Alignment

Broad defense partnerships across the Indo-Pacific and European-Atlantic regions reinforce interoperability and security cooperation in space.

Australia has long been a key U.S. ally. The AUKUS pact among Canberra, London and Washington originally focused on delivering advanced technology and nuclear-powered, conventionally armed submarines. Australian proposals to expand AUKUS into space cooperation reflect the nation's interest in deeper integration with U.S. space security efforts.

> **"We are building a coalition capable of addressing the challenges of a contested space environment. To be effective, we must collaborate on our architectures, integrate our training, exercises and operations, and build a common understanding of the threats we face."**
>
> **~ Gen. B. Chance Saltzman**
> U.S. Space Force Chief of Space Operations

Beyond AUKUS, Australia participates in multinational space operations and contributes geographic advantages, such as sensor locations in the Southern Hemisphere that enhance global tracking and space domain awareness.

Canada's space collaboration with Allies and Partners has endured for decades, supported by defense and intelligence ties. A founding member of the CSpO, Canada is intensifying defensive and offensive space capabilities, Brig. Gen. Christopher Horner, commander of the Canadian Armed Forces Joint Force Space Component, told The Japan Times newspaper.

Like Australia, Canada is a member of Operation Olympic Defender, a multinational force to integrate military space power, enable combined forces, deter aggression and, if necessary, defeat adversaries. With members also including France, Germany, New Zealand, the U.K. and the U.S., the force declared initial operating capability in 2025.

Multinational military personnel attend a briefing during exercise Global Sentinel in April 2025.
DAVID DOZORETZ/U.S. SPACE FORCE

Exercise Global Sentinel participants discuss space scenarios at Vandenberg Space Force Base, California, in May 2025.
DAVID DOZORETZ/U.S. SPACE FORCE

"A year ago, we didn't say the words 'space control' out loud because that was a classified thing. ... But today I can say that those seven nations are certainly all moving towards expanding their capabilities in the space control realm," Horner said in November 2025.

Japan and South Korea are vital U.S. allies in the Indo-Pacific with defense ties that increasingly emphasize space cooperation. Japan is a founding partner in the Artemis program, which will send astronauts to the moon for the first time since 1972 and build a foundation for human exploration to Mars. U.S. Space Forces-Japan activated in 2024 to support partnership agreements with Tokyo, deepen integration with Japanese space counterparts and meet dynamic regional challenges for a free, open and prosperous region.

South Korea's expanding space capabilities — including planned satellite constellations compatible with the U.S. Global Positioning System and Artemis Accords commitments — further illustrate how interoperability extends to Indo-Pacific partners.

While Taiwan does not have a formal space defense alliance, recent U.S. moves to deepen technology cooperation suggest expanding collaboration in space-related areas. Taipei's capabilities in semiconductor technology, electronics manufacturing and satellite development complement U.S. efforts to build interoperability and resilience across a wider constellation of partners.

European partners are integral to multinational space security initiatives. The U.K. and the U.S. routinely conduct combined space missions, such as the 2025 coordinated satellite maneuver during Operation Olympic Defender. "We are now, with our allies, conducting advanced orbital operations to protect and defend our shared national and military interests in space," Maj. Gen. Paul Tedman, commander of the U.K. Space Command, said after the exercise.

Meanwhile, the European Union is exploring

cooperative satellite networks with Japan, leveraging shared standards and joint ventures that could further enhance interoperability across regions.

The U.S. continues to engage with nations on space security issues, even as geopolitical competition grows. Through international treaties and diplomacy, Washington seeks to maintain dialogue aimed at preventing conflict in orbit. China, Russia and the U.S. all signed the United Nations-backed Outer Space Treaty, which in 1967 formed the basis of international space law. It establishes that outer space should be used for peaceful purposes and prohibits placing nuclear weapons in orbit. U.S. officials frequently point to the treaty as a cornerstone of global efforts to keep space secure and stable.

Engagement with China has included a bilateral dialogue on space security. Civil space cooperation between Russia and the U.S. has continued for decades, as exemplified by the International Space Station (ISS). Even amid tensions, the nations rely on each other to operate the orbiting laboratory. Both countries' spacecraft transport crew members to the ISS while U.S. systems power the station and Russian thrusters maintain its altitude.

Interoperability in Action

Space defenders from NATO members and 29 partner nations — including Australia, Canada, Japan, New Zealand, South Korea, Thailand, the U.K. and the U.S. — embedded in regional space operations centers in April and May 2025 to rehearse maintaining national command and control of their sensors for planning, tasking and analysis. Exercise Global Sentinel simulations mirrored the platforms used for real-world space defense.

Three months later, nine partner nations tested strategies, evaluated technology and strengthened space cooperation with the Schriever Wargame at the U.S.'s Maxwell Air Force Base in Alabama. "Every time we come together, the domain looks different — new technologies, new commercial players, new dynamics," said Justin Boileau, the 3 Canadian Space Division chief of advanced effects. "That makes it even more important to work together toward a common understanding so that everyone can benefit from space." The wargame's 2025 iteration also included Australia, France, Germany, Italy, Japan, New Zealand, Norway, the U.K. and the U.S. Planning is underway for Schriever Wargame 2027, where partner nations are expected to jointly set objectives for the first time.

Meanwhile, planners routinely incorporate the space domain in multilateral exercises including Cobra Gold in Thailand, Balikatan in the Philippines and Talisman Sabre in Australia. Such training unites partner militaries to address space security issues, share tactics and procedures, and enhance mutual understanding of complex threats, broadening interoperability and strengthening collaboration.

Partner-Driven Future

Through CSpO, exercises such as Global Sentinel and the Schriever Wargame, and the International Partnership Strategy, the U.S. avoids imposing a unilateral framework for space. Instead, Washington seeks to co-construct a coalition of nations with shared values for mutual benefit. Allies and Partners bring unique strengths — from Australia's geographic advantages to Pacific partners' forward presence — that collectively enhance space security more than any single nation could provide.

U.S. Space Force Guardians at the Combined Space Operations Center at Vandenberg Space Force Base coordinate, plan and execute operations around the clock. DAVID DOZORETZ/U.S. SPACE FORCE

Challenges include disparities in technology, doctrine and funding. Balancing defense imperatives with civil space goals, such as scientific exploration and economic expansion, will require diplomacy. Strategic competition also affects coalition-building in the space domain.

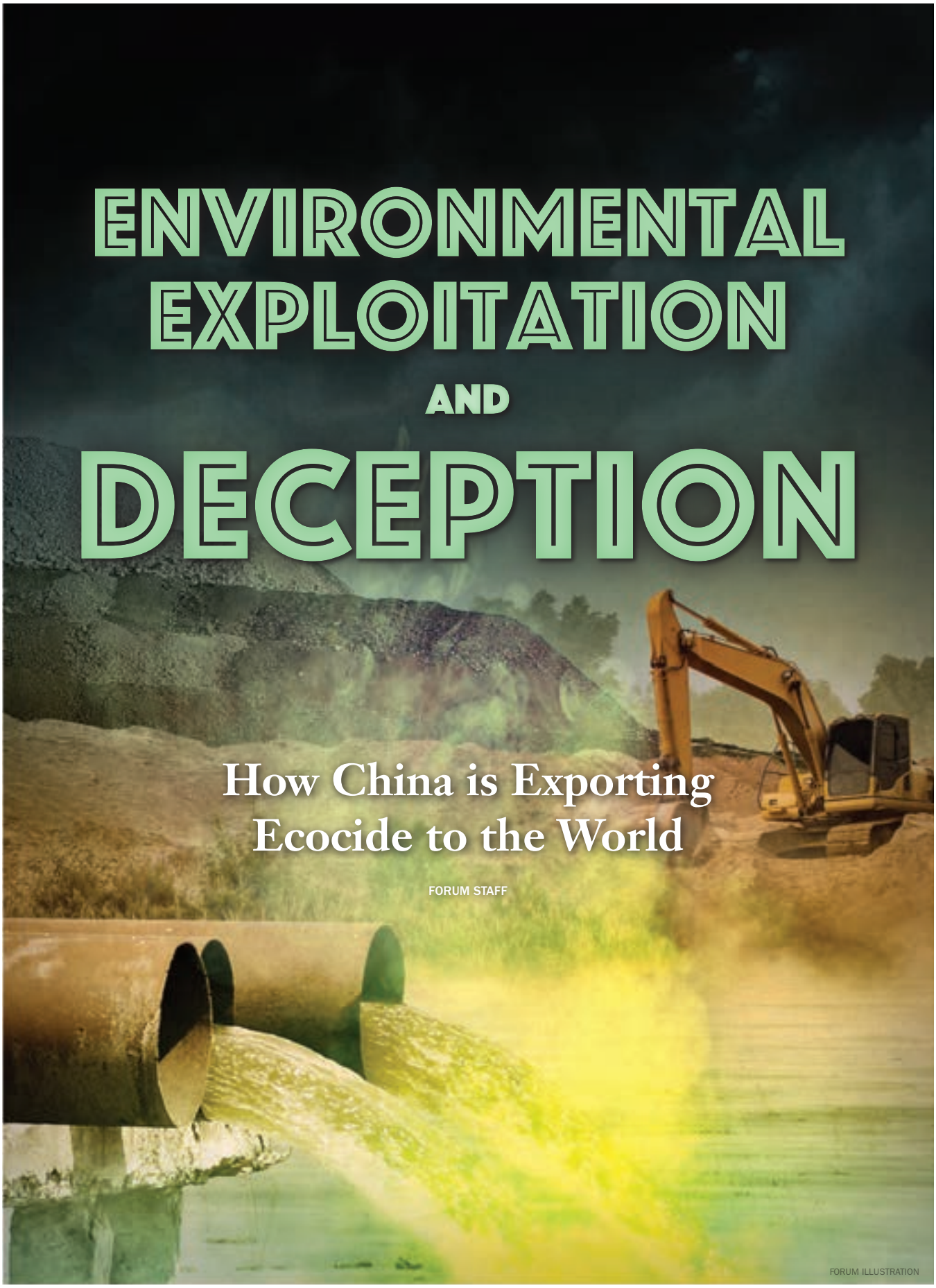
The U.S. Space Force's International Partnership Strategy reflects a shift in how space security is conceptualized and operationalized. Allies and Partners reject unilateral control of the vital domain in favor of building a resilient, interoperable coalition that can deter conflict, share information and respond collectively to threats.

Interoperability — in data, operations and strategic planning — lies at the heart of this approach. By weaving together global capabilities, the U.S. and its Allies and Partners are shaping a collective security architecture in space that supports freedom of access and responsible conduct. □

ENVIRONMENTAL EXPLOITATION AND DECEPTION

How China is Exporting Ecocide to the World

FORUM STAFF



FORUM ILLUSTRATION

The Kok River flows through Chiang Mai province after entering Thailand from Myanmar, where unregulated rare-earth mining releases toxic chemicals into the water. REUTERS

Beijing has increasingly attempted to brand itself as a global leader in protecting the environment and providing clean energy and sustainable development. Yet underneath that propaganda lies a dark reality: China is exporting some of its worst environmental practices to developing nations through aggressive investments and resource-extraction campaigns, especially in critical minerals and raw-material industries. The result: widespread ecological destruction, toxic pollution and long-term damage to fragile ecosystems across Southeast Asia and beyond.

Examples range from nickel mining in Indonesia and rare-earth mining in Myanmar to steel and paper mills across the region, indicating a pattern of exploitation that starkly contrasts China's professed environmental stewardship.

A geo-economic and humanitarian challenge is unfolding with implications for regional stability, public health and global security. The international community must develop solutions to China's export of destructive environmental practices.

A Grab for Critical Minerals

As demand surges for electric vehicles (EV), renewable energy technologies and advanced electronics, the race for battery metals and rare-earth elements has intensified. Despite already being a processing leader, China has steadily expanded its reach by relocating the dirtiest, most polluting parts of its supposedly green supply chain, often to countries with weak environmental governance, lax enforcement or ongoing conflicts.

Many of the targeted countries, such as Indonesia, Laos and Myanmar, are strategically important for China under the framework of its hegemonic One Belt, One Road scheme. Beijing presents its infrastructure, smelters and industrial parks as investment or aid — but the underlying motive is resource control and profit, often at the cost of local health, ecology and sovereignty.

In Indonesia, which has the world's largest nickel reserves, Chinese firms, notably Tsingshan Holding Group and Jiangsu Delong Nickel Industry Co., control about 75% of nickel refining capacity, the United States-based global security nonprofit C4ADS reported in February 2025.

"A lack of domestic control leaves Indonesia reliant upon Chinese investment and continued support of the industry, which may limit the government's ability to hold the industry accountable and shape the sector for its own economic benefit," C4ADS reported.

Meanwhile, in Myanmar's border regions, such as Shan and Kachin states, Chinese state-affiliated mining firms have ramped up rare-earth extraction, often operating under little or no regulatory oversight due to the protracted civil war, reported the Thailand-based news website The Nation.

China's pattern of expansion suggests a deliberate strategy: secure access to critical resources cheaply and at scale, while outsourcing the environmental cost to states with weaker regulatory capacity or greater political vulnerability.

Nickel in Indonesia: The Price of Batteries

Nickel is essential for stainless steel and EV battery production. But the way China's nickel sector has expanded in Indonesia, particularly with coal-powered smelters and processing plants, has caused severe environmental and social damage, experts contend.

China has supported this expansion through predatory financing of the massive Indonesia Morowali Industrial Park (IMIP) on Sulawesi and other smelter clusters on Halmahera. Many of these facilities run on captive coal-fired power plants, even as their output feeds supposed clean-energy supply chains abroad.

IMIP is expected to have an annual coal-fired power capacity of 5 gigawatts, or nearly as much coal power as Mexico generates each year, according to advocacy group Mighty Earth. In addition to high emissions, these coal plants pollute the air, water and land, threatening local livelihoods, the Asia Pacific Solidarity Network reports.

A worker supervises slag disposal from a nickel ore processing factory in South Sulawesi, Indonesia, in August 2024.
REUTERS

Deforestation has been extensive. Since 2000, over 8,700 hectares of rainforest have been cleared in the North Morowali region alone to make way for mines, smelters and infrastructure, according to environmental groups including Greenpeace Indonesia. This massive land conversion has destabilized local ecosystems, undermined watershed integrity and degraded habitat for biodiversity. Agricultural land and water sources vital to local communities have been disrupted, the groups report.

The pattern extends beyond Indonesia. In Papua New Guinea, testing at a Chinese-operated nickel mine revealed contamination patterns strikingly similar to those in Indonesia: inadequate containment systems, toxic runoff threatening communities and ecosystems, and dangerous levels of heavy metals, including hexavalent chromium, a carcinogen. Multiple contaminants exceed safety standards by orders of magnitude, demonstrating Chinese firms are systematically replicating harmful practices across the Pacific, according to a U.S. government analysis.

Polluted water stagnates near nickel mining activities that surround Baliara village on Kabaena Island in Southeast Sulawesi, Indonesia, in November 2024.
THE ASSOCIATED PRESS

Pollution, Worker Deaths, Social Costs

The environmental toll is matched by alarming social costs. Chinese-backed nickel smelters in Indonesia were frequently accused of air and water pollution, soil contamination and biodiversity loss, according to a 2023 report by the London-based advocacy group Business and Human Rights Centre. The report, "Unpacking clean energy: Human rights impacts of Chinese overseas investment in transition minerals," covered 18 countries with the Democratic Republic of the Congo, Indonesia, Myanmar, Peru and Zimbabwe recording the highest numbers of allegations.

At the same time, labor conditions in Indonesia have been repeatedly criticized as unsafe and exploitative. Between 2015 and 2023, more than 90 deaths and 100 injuries were reported in processing facilities there. In 2023, at least 60 deaths or serious accidents were linked to Chinese-owned smelters, including a fire at a Tsingshan-owned facility that killed 21 people and injured 38, according to Mongabay, a conservation and environmental science news platform.

Pollution and wastewater runoff have decimated fish populations, destroying livelihoods of people rely on fisheries and marine resources, environmental groups report.

Underlying many of these abuses are corruption and weak enforcement. Roughly one-third of over 330 nickel mining and refining projects in Indonesia had been accused of corruption or illegal mining, according to a 2024 investigation by the China Global South Project, a nongovernmental organization.

"Corruption and environmental damage in Indonesia's nickel industry have become closely linked: when a nickel mining company operates illegally, the local community and ecology tend to suffer," the report said. "The widespread Chinese financing of the Indonesian nickel industry seems to have led some to grow wary of Chinese investors and their relationships with local officials, since local governments have been broadly criticized for corrupt business dealings."

Although the report cites China for the growth of Indonesia's nickel mining industry, the expansion has negative consequences. What is promoted as foreign investment or industrial development often translates into a de facto resource grab, with environmental safeguards sacrificed for profits and speed.

Myanmar's Mining and the Mekong Crisis

China's drive to dominate rare-earth resources is matched by its readiness to outsource environmental harm to unstable frontier zones.

Historically, China conducted much of its rare-earth extraction within its borders. But domestic environmental and health concerns, especially contamination of soil and groundwater, led Beijing to shutter hundreds of small

Thai pollution control officers collect samples from the Kok River in November 2025 to test for heavy metal contaminants, including arsenic. REUTERS

private mines after 2011, according to a June 2025 report in Le Monde, a French newspaper.

Rather than cleaning up heavily polluted sectors at home, including nickel smelting, rare-earth mining and heavy industry, China began relocating them. Beijing is recasting what was once a domestic problem as a so-called foreign development opportunity, Le Monde reported.

The cost of producing heavy rare-earth elements such as dysprosium and terbium, both used in advanced weapons systems, is one-seventh the price in Myanmar than in China, according to Benchmark Mineral Intelligence, a London-based market research firm. To meet demand, China redirected extraction to neighboring Myanmar, particularly to conflict-affected territories in Shan and Kachin states. These regions, under the sway of ethnic armed organizations or remote military outposts, offer lax oversight and minimal accountability.

Satellite imagery shows explosive growth: mining sites, road networks and waste ponds cutting into once-untouched hillsides, according to the Shan Human Rights Foundation. These mines extract key rare-earth elements for export to China.

At least a dozen gold and rare-earth mines were established in southern Shan in 2025 alone, according to Zachary Abuza, a professor at the National War College in Washington, D.C.

Myanmar's civil war has persisted for more than five years, producing a lawless border area mainly held by ethnic armed groups. Chinese firms operate via informal networks, often in alliance with the military junta as well as local militias or armed groups, making accountability nearly impossible, Abuza told the Al Jazeera news agency.

"In this vacuum, mining has exploded — likely with Chinese traders involved. The military in [Myanmar's capital] Naypyidaw can't issue permits or enforce environmental rules, but they still take their share of the profits," he said.

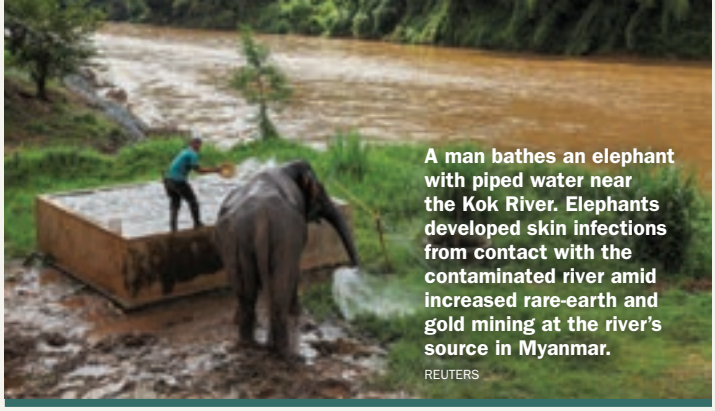
In a November 2025 report, the Stimson Center think tank used satellite imagery to identify 2,420 unregulated mining sites on major river systems in Cambodia, Laos and Myanmar. "Over the last decade, a boom in unregulated mining has been sending dangerous contaminants such as cyanide, mercury, arsenic, and other heavy metals directly into scores of rivers throughout mainland Southeast Asia," the report stated.

"Since the mining operation started [in Myanmar], there is no protection for the local people," Sai Hor Hseng, a spokesman for the Shan Human Rights Foundation, which is based in the eastern Myanmar state, told Al Jazeera. The mining companies "don't care what happens to the environment," he said, or to those living downstream in Thailand.

Continued on Page 58

China's Export of Harmful Mining Practices Exacerbates Regional Pollution

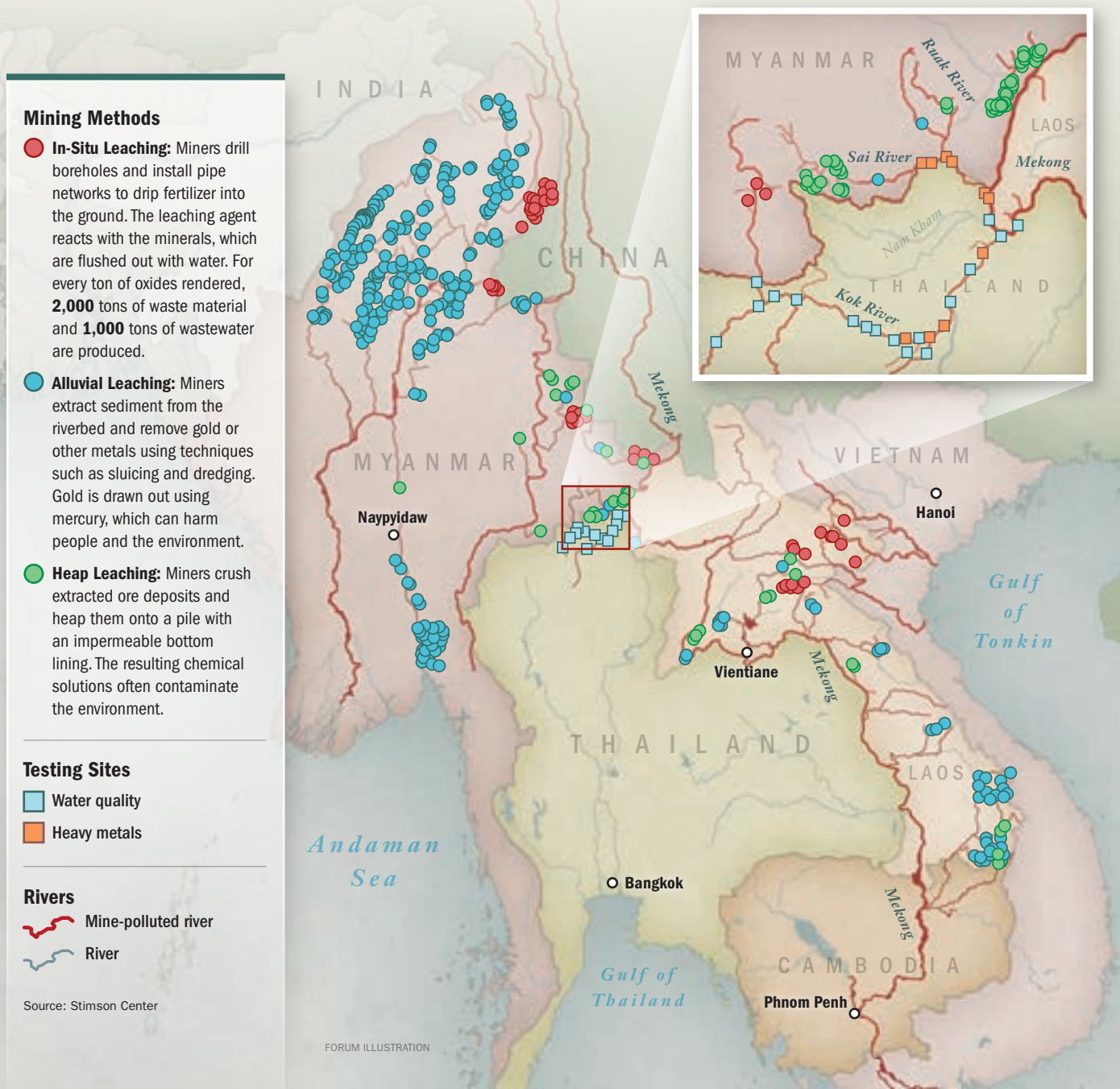
China's aggressive investments and resource mining pursuits, especially of rare-earth minerals, are accelerating environmental degradation across Southeast Asia and beyond.



A man bathes an elephant with piped water near the Kok River. Elephants developed skin infections from contact with the contaminated river amid increased rare-earth and gold mining at the river's source in Myanmar.
REUTERS

Mekong River Tributaries Poisoned by Unregulated Chinese Mining

A boom in unregulated mining in the past decade has released arsenic, cyanide, mercury and other contaminants into rivers across Southeast Asia. Satellite imagery revealed more than **2,400** sites for unregulated in-situ leach (rare earth), heap leach (gold, copper, nickel, manganese) and alluvial mining (gold, silver, tin) on or alongside **43** rivers in Myanmar, Laos and Cambodia. Nearly **800** of the sites are along Mekong tributaries. China is driving much of this surge, given the cost of producing rare-earth elements such as dysprosium and terbium, both used in advanced weapons systems, is one-seventh the price in Myanmar than in China, according to Benchmark Mineral Intelligence. Locations affected by Myanmar's prolonged civil war, such as Shan and Kachin states, seem especially susceptible to such exploitation.



Case Study: China's Exploitation of Indonesia's Key Resources

Nickel Mining Nexus

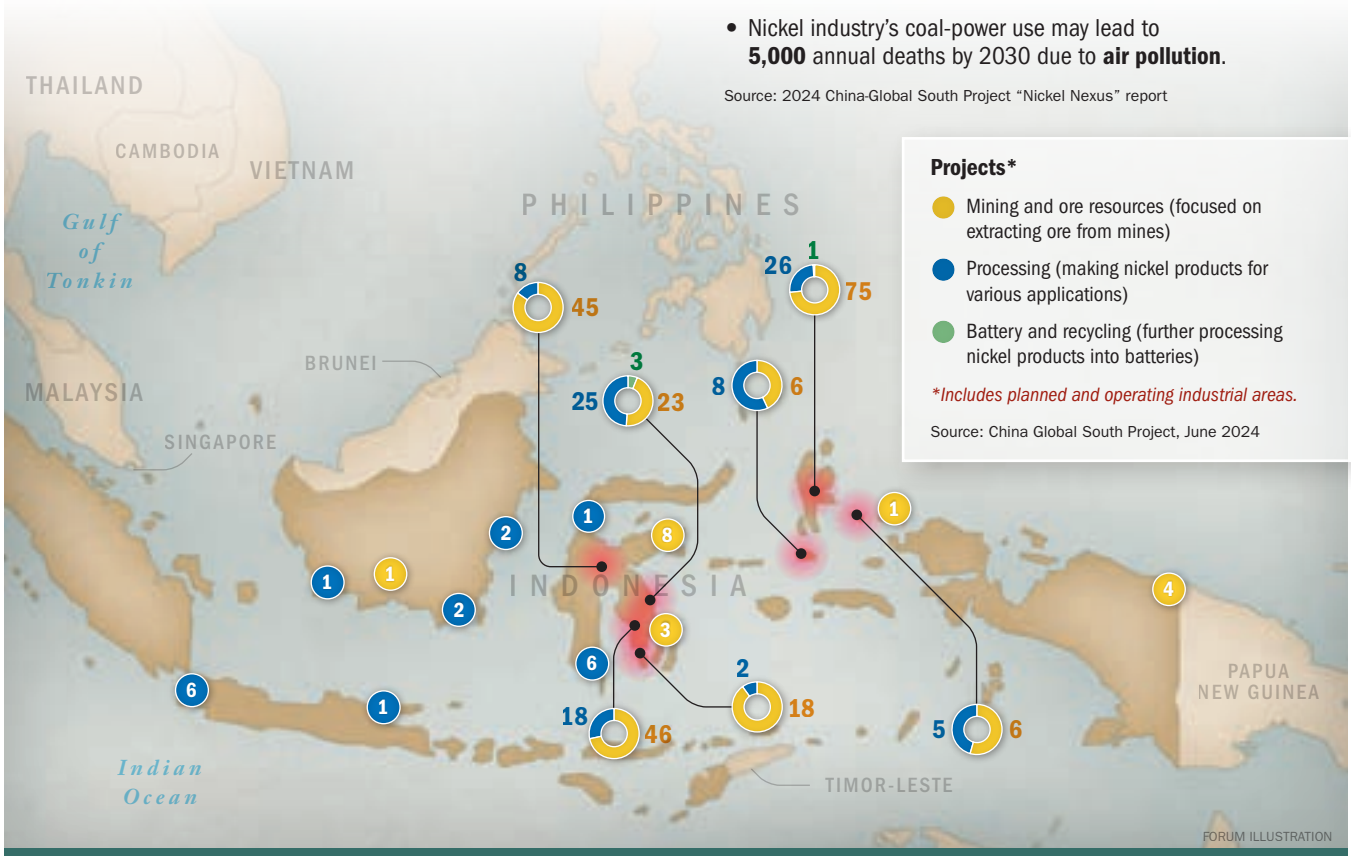
Indonesia is the world's largest nickel ore supplier, providing about half of global demand in 2023. Chinese companies own about **90%** of Indonesia's nickel processing facilities, and China accounts for up to **70%** of all investments in Indonesia's nickel industry, according to government officials. China's entrenched role in Indonesia's nickel sector has contributed to the proliferation of practices that exploit local communities and the environment.

MINING AND PROCESSING PROJECTS

350+ projects studied; **$70.2 billion** in investments

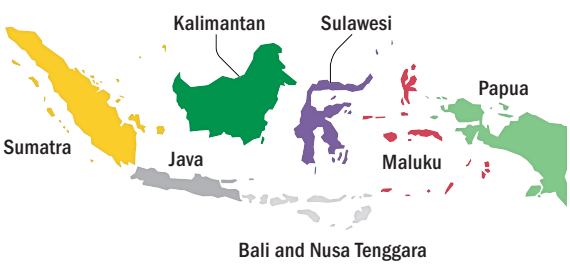
- Chinese shareholders control at least **75** of some **350** projects studied.
- More than one third of projects were accused of or involved in corruption or **illegal mining**.
- **Water pollution** is the top concern for villagers living near nickel mines and factories.
- Nickel industry's coal-power use may lead to **5,000** annual deaths by 2030 due to **air pollution**.

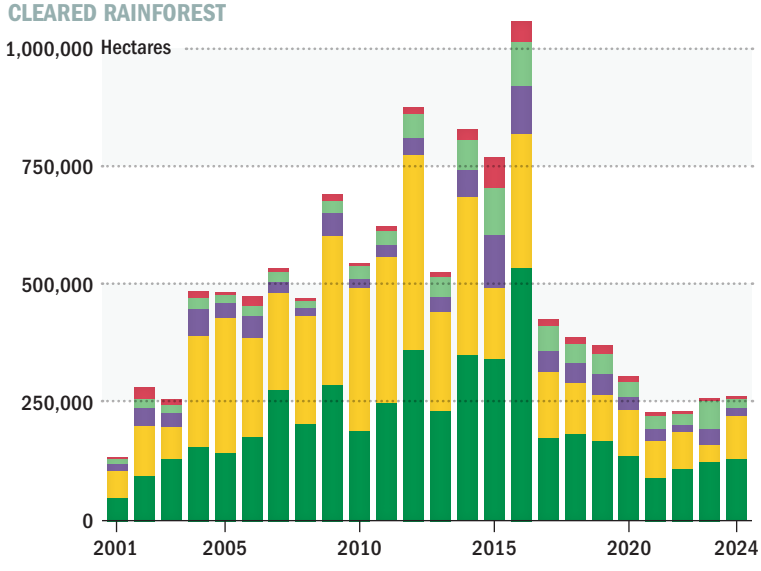
Source: 2024 China-Global South Project "Nickel Nexus" report



Deforestation in Indonesia

In addition to causing pollution through mineral extraction and processing practices, the pursuit of critical minerals has accelerated deforestation. Since 2000, for example, over **8,700** hectares of rainforest have been cleared in Indonesia's North Morowali region in Sulawesi alone to make way for mines, smelters and infrastructure.





Source: worldenergydata.org

Reversing Environmental Degradation Caused by China

China's exportation of harmful mining practices can be reduced by international enforcement of environmental and social standards and by increased coordination among the United States and its Allies and Partners.

The following measures can mitigate environmental damage, minimize future damage, curtail China's harmful practices and protect vulnerable populations and lands from abuses linked to global demand for critical minerals.

Promote Alternative Supply Chains, Strict Standards

- **More countries could invest in domestic mining and processing capacity** or in recycling critical minerals, under stricter environmental standards, reducing reliance on China-dominated supply chains.
- **Support mining and processing operations that adopt best practices,** such as promoting wastewater treatment, responsible waste management and reforestation, rather than enabling the lowest-cost, highest-pollution model.

Support Regulatory Capacity, Governance in Host Countries

- **International organizations such as the United Nations and development banks should provide financial, technical and institutional support** to strengthen environmental regulation, monitoring and enforcement in developing countries.
- **Civil-society organizations, local communities and media must be empowered to monitor, report** and hold investors and governments accountable.

Promote Supply Chain Transparency

- **Use technology, including satellite monitoring, blockchain-based supply-chain tracing and remote sensing,** to detect illicit mining, deforestation, pollution and waste mismanagement.
- **Publish data on ownership, financing, environmental assessments, pollution incidents and compliance** so companies, regulators and the public know who is responsible and where.

Strengthen Environmental, Human Rights Requirements

- **Governments, multilateral institutions and investors in allied and partner nations should demand** that companies sourcing minerals or materials from abroad conduct rigorous environmental and social due diligence, covering not only mines and smelters but also supply-chain impacts and downstream pollution.
- **Host nation governments also should enforce licensing,** environmental impact assessments and community consultation, and ensure transparency.

Apply Economic Pressure

- **Nations and trading blocs should adopt policies and regulations** that consider environmental impact and responsible sourcing, including for EVs, electronics and renewables.

Continued from Page 55

Transboundary Pollution

The environmental harm is not constrained within Myanmar's borders. Toxic runoff, including heavy metals and arsenic, has polluted the Kok River and its tributaries, which feed into the Mekong, threatening water supplies, fisheries and farming communities in northern Thailand, Laos and farther downstream.

Arsenic levels in parts of the Kok River and Mekong tributaries exceeded by as much as 40 times the levels defined as safe by health authorities, the Thailand-based CTN News portal reported in August 2025. Local communities report fish deformities and die-offs; farmers fear their crops will absorb toxins; residents have developed skin ailments after contact with contaminated water, all "traced to upstream mining operations" across the border in Shan, according to the Bangkok Post newspaper. Elevated arsenic levels also have been found in the Mekong.

The contamination potentially affects tens of millions of people across Southeast Asia. Downstream impacts of such mining ripple across borders, contaminating rivers, agricultural land, fisheries and communities in neighboring countries such as Laos and Thailand.

The cross-border pollution crisis is severely impacting millions of people in Chiang Rai in northern Thailand, who face risks to their livelihoods and health due to heavy metal contamination, particularly arsenic, in the Kok River, which flows into the Mekong and Sai rivers, Pianporn Deetes, director of Southeast Asia Campaigns at International Rivers, told the Bangkok Business newspaper.

"Local residents can no longer engage in traditional activities like fishing or operating tour boats, and farmers are worried that rice grown using water from the Kok River may be contaminated with arsenic, as rice tends to absorb arsenic well. Additionally, there have been reports of fish with unusual parasites, which correlate with mining activities disturbing the soil," Deetes said.

Ben Hardman, Mekong legal director for the advocacy group EarthRights International, told Al Jazeera in August 2025 that residents worry that Shan and neighboring countries into which Myanmar's rivers flow will suffer the same fate as Kachin, especially if rare-earth mine sites multiply to meet growing global demand.

"There's a long history of rare-earth mining causing serious environmental harms that are very long-term, and with pretty egregious health implications for communities," Hardman said. "That was the case in China in the 2010s, and is the case in Kachin now. And it's the same situation now evolving in Shan state, and so we can expect to see the same harms."

The pattern extends globally. Testing at Chinese-operated mining and refining facilities across the Pacific, Africa, Latin America and the Caribbean reveals the same systematic failures: adverse levels of mine waste, inadequate containment, and contamination

Excavators load trucks with rare-earth minerals at a mine in southwest China's Yunnan province in 2008. China is exporting its destructive mining practices to vulnerable countries, experts say. REUTERS

threatening water supplies and communities. Regardless of commodity or location, Chinese firms prioritize profit extraction over environmental protection, leaving host nations to bear the costs of pollution and ecological damage.

Steel, Paper Production

China's resource grab doesn't stop at raw materials. Through investment, Chinese firms have exported steel production, paper mills and plantations to Southeast Asia and elsewhere in the Indo-Pacific, often bringing pollution-intensive technology, weak regulation guidelines and environmental degradation.

With pressure on domestic heavy industry mounting, such as stricter regulations, expansion limits and carbon-emission targets, many Chinese steel producers, for example, are shifting to Southeast Asia and beyond. As of 2023, China accounted for about 80% of total foreign investment in new steel capacity in Southeast Asia, according to a 2025 report by Agora Industry, a Germany-based think tank.

Most of these plants rely on older, coal-fired furnace technology, which produces the most harmful emissions, particulate matter and local pollution, Agora reported. The results are rising carbon emissions regionwide as well as local air and water pollution, strain on ecological systems, and deteriorating public health. Moreover, the flood of cheap Chinese steel into Southeast Asian markets undermines local producers, discouraging investment in cleaner and more environmentally responsible steel production, the SteelRadar website reported. Chinese-backed smelting companies in Indonesia, including Tsingshan Holding Group and PT Obsidian Stainless Steel, have been linked to air pollution, contaminated water systems, fisheries damage and deforestation, according to a 2026 report on the Dhaka Tribune website.

The world has observed similar patterns in China's pulp-and-paper sector. In recent decades, China's growing demand for timber and paper has driven massive plantation and logging operations in Southeast Asia. Large-scale concessions for pulpwood plantations have spread across Cambodia, Laos, Myanmar and Vietnam, often at the cost of natural forests, biodiversity and local land rights, according to the Wilson Center, a U.S.-based think tank. China's Sun Paper Group, for example, has drawn criticism in the past decade for its paper mill operations in Laos that allegedly contaminated water, reduced agricultural quality and polluted nearby communities, causing illness among residents, according to news reports.

China-linked paper companies often acquire pulp from Southeast Asian plantations, effectively externalizing environmental degradation while reaping profits and meeting global demand. Communities displaced by these plantations lose access to forest resources; traditional agriculture and livelihoods are disrupted.

Despite China's efforts to create a more sustainable domestic pulp-and-paper sector, its overseas supply chain — where timber is felled, plantations expanded and forests razed — remains a glaring contradiction to Beijing's "green paper" narrative.

Strategic, Moral Leadership

Supply chain dominance in critical minerals and metals confers China with strategic leverage over industries from consumer electronics to defense. Yet evidence strongly suggests that Beijing is using its might not to build a sustainable future, but to export environmental destruction to some of the world's most vulnerable communities, including many in Southeast Asia.

The international community, including governments, investors, multilateral institutions and civil society, must confront this reality. Transparency, accountability and enforceable standards are needed to prevent China's exploitation in the name of clean energy, advocates say. Otherwise, emerging economies will be left with toxic landscapes, broken communities and ecological collapse while China prospers. Only by confronting such predation and holding all stakeholders accountable can peace, security and prosperity be ensured in the region. □

Source: ResearchGate.net
FORUM ILLUSTRATION

REMOVING BARRIERS, SHARING SOLUTIONS

Trust, Interoperability and Mutual Purpose are Critical to First Island Chain Partnerships

LT. COL. KEVIN M. WHEELER/U.S. MARINE CORPS

Promoting peace and stability in the Indo-Pacific hinges on strategic depth. Resilient relationships are born of shared visions and coupled with interoperable strategies able to adapt as conditions change. Plans must be designed not for short, intense skirmishes but for prolonged struggles over influence, access and values. A mindset that prioritizes long-term coalition strength over short-term lethality will secure a free, secure and prosperous Indo-Pacific.

The United States and its Allies and Partners must operate from a position of strength. Success will be built on a foundation established by like-minded stakeholders working together. National commitments and mutual trust among partners are essential. As the saying goes, "If you want to go fast, go alone. If you want to go far, go together." To embrace inevitable challenges, the U.S. and its Allies and Partners must emphasize the enduring strategic value of the first island chain, the strand of archipelagoes off Asia's east coast that includes Brunei, Indonesia, Japan, Malaysia, the Philippines, Taiwan and Singapore, which poses a hurdle for any revisionist power seeking Pacific Ocean access.

Mutual trust, access and shared interests are critical to ensure the stability and security of not only the first island chain but also the entire Indo-Pacific. Allies and Partners must clearly explain why securing first island chain nations and territories is vital, making their case concisely and judiciously and deploying personnel and resources

when needed. In the digital age, when information can move faster than a hypersonic missile, effective messaging will aid this effort.

Our Word Is Our Bond

U.S. mutual defense treaties such as those with Japan and the Philippines are more than legal obligations; they are promises of solidarity based on trust. From an armed forces perspective, supporting Allies and Partners means ceding some operational independence for the collective benefit.

Weapons sales, interoperability and, in some cases, interchangeable hardware are key. Japan deploys U.S.-designed and manufactured weapons such as fighter aircraft, missiles and naval combat systems. Japan also supplies the Philippines with defense technology such as a command and control system. Partner forces routinely participate in bilateral and multilateral military exercises.

Removing barriers to procuring high-performing technologies from foreign suppliers is spurring unprecedented collaboration. It enables the integration of commercial supply chain management practices and puts sustainment requirements closer to points of need. This trend must continue to grow.

Shared needs — basic logistics, housing, food, water — can be met with shared solutions. The goal must be a trusted, interoperable network of Allies and Partners anchored by shared access, logistics and supply chains.

Armed forces increasingly are improving efficiency with artificial intelligence tools that synthesize vast data streams and replace siloed systems specific to individual services and functional areas. Allies and Partners must establish secure distributed data systems that allow information to flow across borders and domains, enabling like-minded nations to support one another. Coalition logistics and infrastructure require integrated data systems that help commanders plan and rehearse possible scenarios, accelerating decision-making and ensuring best use of finite resources.

Enduring Influence

Combined efforts to promote peace and stability must be enduring. This is where defense forces play a stabilizing role through presence, posture and partnership. Force engagement, aligned with diplomatic, informational and economic initiatives, provides continuity and signals long-term commitment. To strengthen this architecture, Allies and Partners must:

- Continue developing metrics of effectiveness beyond kinetic outcomes. This could include the ability of coalition forces to seamlessly operate multiple units, sustain combat operations because of pre-positioned stocks and accurately predict sustainment shortfalls based on superior data analysis.
- Enhance training pipelines for regional expertise and language skills. Allies and Partners must familiarize service members and public servants with a country or region, allowing them to build relationships, understand geography and embrace host nation cultures.
- Promote interagency coordination for a whole-of-government approach, creating structured forums within each country to facilitate sustained collaboration.

Encouraging long-term stability requires continuous engagement, shared planning and scalable participation among coalitions, anchored by person-to-person relationships.

Establishing influence in the Indo-Pacific takes generations. Success will be measured in trust, interoperability and shared purpose. A foundation built on coalitions with resilient physical and digital architecture will allow nations to outlast long-term challenges and outmaneuver short-term threats. This is a template for enduring influence, one that prioritizes relationships over reaction, presence over rhetoric and coalitions over artificial timelines. □

Japanese, Philippine and United States forces train in the South China Sea in March 2025. THE ASSOCIATED PRESS

Taiwan Soldiers conduct a live-fire drill in Hsinchu County in July 2025. THE ASSOCIATED PRESS

RESPONSIBLE PARTNER

THE PHILIPPINES' FORMER MILITARY CHIEF REFLECTS ON CHALLENGES FACING THE NATION AND THE POWER OF PARTNERSHIP

Philippine Marines conduct ambush drills during Exercise Balikatan on the Philippines' Batan Island in April 2026.
SGT. IYER RAMAKRISHNA/U.S. MARINE CORPS

FORUM STAFF

In a time of rapidly evolving security challenges, the Armed Forces of the Philippines (AFP) is navigating complex traditional and nontraditional threats while expanding and reinforcing partnerships across the Indo-Pacific and beyond. After becoming AFP chief of staff in July 2023, Gen. Romeo Brawner Jr. led the multidomain transformation and overseen an expansive military modernization that has positioned Manila as a key strategic partner in upholding peace and stability in Southeast Asia and the wider region.

Gen. Brawner retired in July 2026 after a highly decorated military career spanning more than three decades. A native of Baguio, a city in the Philippines' northern island of Luzon, he graduated from the Philippine Military Academy in 1989. Prior to leading the AFP, he was the Philippine Army's 65th commanding general. He also served as chief of the 6th Special Forces Company and 2nd Special Forces Battalion, operations officer in the Special Forces Regiment, chief of the Army's 6th Infantry Division, and commander of the Civil-Military Operations Regiment.

LEFT: Gen. Romeo Brawner Jr., then Armed Forces of the Philippines (AFP) chief of staff, speaks during the AFP's 88th anniversary at Camp Aguinaldo in Quezon City in December 2023. THE ASSOCIATED PRESS

Adm. Samuel J. Paparo, Commander of United States Pacific Command, right, presents Gen. Brawner with the Legion of Merit, Degree of Commander, in May 2026 in recognition of his strategic leadership, operational excellence and exceptional service. STAFF SGT. ANGEL HERALDEZ/U.S. ARMY

Gen. Brawner has master's degrees in information management, business administration and strategic studies. He was inducted into the United States Army War College International Fellows Hall of Fame in 2023 and awarded the Legion of Merit, Degree of Commander, for exceptional service.

As he looks toward new opportunities to serve his country, Gen. Brawner spoke with FORUM about internal and external security threats facing the Philippines, including the flash point of the South China Sea; the nation's growing role in multilateral engagements with Southeast Asian neighbors and partners including Australia, Japan and longtime ally the U.S.; emerging domains such as cyber and space; and the increasing importance of joint exercises, intelligence sharing and preparedness.

"We believe that no single country can defend itself [alone], especially against the threats that we are facing now," he said.

FORUM: What are the Philippines' primary security concerns?

Gen. Brawner: What concerns us the most is internal security operations. We are hoping that by the end of 2026 we will have eliminated all terrorist groups and there will be no resurgence. Externally, our main concern is to ensure we contain China's expansionist objectives. Right now, we are focusing on Bajo de Masinloc [Scarborough Shoal] because that is their target. We have to prevent them from gaining full control or even establishing facilities there. Once they are able to establish a facility, that's it, that's the end. We will not be able to reclaim it … they will be able to control the whole South China Sea.

FORUM: What is the Philippines' role in its trilateral partnership with Japan and the U.S., and the defense grouping known as the Squad, which also includes Australia, Japan and the U.S.? How have these partnerships enhanced security and what lies ahead?

Gen. Brawner: Our role is to be a responsible partner. The assumption is that once we enter into minilateral or multilateral arrangements with other countries, we are on equal footing. Despite the advancement in technology or the advancement in their respective armed forces, we all have an equal standing. Whatever it takes to be a responsible partner, we have to do that. For instance, during multilateral maritime cooperative activities, because we are all partners, we have to contribute our share.

The new nontraditional threats — for instance, cyber, information, cognitive, space — all of these target several countries at the same time. The solution to that is to collectively address these threats. The best way to do that is to form coalitions, which we are effectively doing. By forming coalitions, you become stronger as a collective group of countries. All contribute to each other's defenses, to each other's deterrence posture.

The way forward is to strengthen the relations by doing more collaborative activities together, by trusting each other more. For instance, by having more

person-to-person exchanges, subject matter exchanges. Our objective is to have an officer embedded in the U.S. Pacific Command. We are just arranging the mechanics. They already have embedded officers from Japan, Australia and other allied nations like New Zealand. We plan also to embed an officer in Japan and Australia. In the same manner, we welcome these countries to be part of a command center, or control center, here in the Philippines. In the Balikatan 2026 exercise, we had not just the U.S. and the Philippines working together in a common command center, or Combined Coordinating Center, but we also had elements from Japan and Australia.

FORUM: What other security partnerships are important for the Philippines?

Gen. Brawner: We've long established Indomalphi [with Indonesia and Malaysia] and Philindo [with Indonesia] to address cross-border issues such as smuggling and human trafficking. Now, we're strengthening ties with India and South Korea. With South Korea, we have already procured a lot of defense items from them — FA-50 [light combat aircraft], KM-450 and KM-250 vehicles, K-3 machine guns, and frigates, corvettes and offshore patrol vessels. Canada is also a key partner, especially since we signed a visiting forces agreement. They're very serious about their Indo-Pacific strategy and are assigning a three-star general to be based in Manila. Their support includes cyber defense, maritime domain awareness and intelligence sharing.

A Philippine Marine scans the horizon during a patrol on West York Island in the South China Sea in mid-2025.
AFP/GETTY IMAGES

FORUM: What are the AFP's priorities for training and modernization?

Gen. Brawner: Priorities are newer technologies like cyber, artificial intelligence and space. Since we already conduct kinetic warfare training through exercises like Balikatan and Salaknib, we focus on high-technology training. We believe that with the state of the modernization that we have now, we can compete with other armed forces, even advanced armed forces when it comes to cyber. Looking at the wars in Ukraine and [the Middle East], we need to develop unmanned and autonomous systems — air, surface and subsurface drones — as well as missiles and missile defense.

FORUM: Can you tell us about the concept known as One Cooperative Effort Among Nations, or OCEAN, and how it's being operationalized?

Gen. Brawner: We have to consider the first island chain [a string of archipelagoes stretching from Japan to Indonesia] as one theater. We now consider this whole area as one where we could cooperate in several aspects: economics, trade, defense, security, information and others. So, it's not just military, but it's a more expanded concept that would define cooperation. One very concrete effort is during disasters and calamities.

Because of this concept, it's now very easy for other countries, especially in the first island chain, to send assistance. This makes it easier for countries like Japan, the U.S. and Australia to provide humanitarian assistance and disaster response operations. If this is put into action, it would be easier for armed forces to coordinate with each other.

FORUM: Tell us about the AFP's plans to establish a space unit.

Gen. Brawner: We are already using space technology, but we don't have our own satellites. We plan to create a space unit, or maybe a space group, that will cater to the AFP's requirements for information coming from space: satellite images, imaging, and the linking of information and communications. Number one is the improvement of our communications through satellite links and satellite imaging, which are necessary for intelligence analysis and operational planning. Even if we don't have our own yet, we already have satellites that we can tap for our needs. We need a dedicated unit that will harness this information and develop that capability so that we will have our own.

FORUM: How would you describe your tenure as AFP chief of staff?

Gen. Brawner: When I came in, we started reorganizing according to the threats that we are now facing. Aside from the traditional domains of warfare — air, land and sea — we now have information, cognitive, cyber and space. In my conversations with my counterparts, almost all armed forces around the world are reorganizing as well. The new technologies that are coming in will define the new character of warfare — drones, cyber, unmanned

Australian Army Soldiers and Philippine Marines rehearse a combined joint force entry near San Vicente, Philippines, during Exercise ALON 2025. AUSTRALIAN DEFENCE DEPARTMENT

systems, autonomous systems. In my first year, we organized the Armed Forces Intelligence Command because we saw the need for the elevation of our intelligence to a strategic level. Initially, because we were facing internal security threats, our intelligence was focused on that — high-value targets from terrorist [groups]. Now we have to study other threat groups outside the country. We have to elevate our intelligence analysis. That's why we have the Armed Forces Intelligence Command.

We also created the AFP Counterintelligence Group because, aside from the traditional threats, we are now facing destabilization efforts from within the country. We have to guard against that. And then the Cyber Command. From a cyber group, we made it into a command. We are really bent on developing our cyber capabilities so that we are not just able to defend, but we will be able to do offensive cyber operations.

We created the AFP Joint Logistics Command because we realized that in order to win a war, you have to sustain the war. Logistics has to be elevated. Next, we created the AFP Civil-Military Operations Command, which will deal with the information and cognitive domains. If you look at the environment now, there is lots of misinformation and disinformation, so we need a unit dedicated to dealing with this cognitive and information warfare. We also created the Strategic Command because we realized that we need a command that is ready to fight threats from outside. It's the same with Japan. It created its Joint Operations Command recently because of that need.

That was what I was able to do — reorganize, establish more capabilities for the armed forces and, in another aspect, we were able to establish closer relations with partner countries. In 2026, as chair of the Association of Southeast Asian Nations (ASEAN), the Philippines also has taken over the leadership of the ASEAN Observer Team in maintaining the peace between Thailand and Cambodia. That is a very important role that we are playing because if we are successful in this aspect, this could set the future for conflict resolution among ASEAN nations. We believe we are writing history by doing that. □

Correspondent Frances Mangosing contributed to this interview, which was edited to fit FORUM's format.

Earthquake Monitors Track Space Junk Through SONIC BOOMS

Scientists used seismic readings from sonic booms to track the reentry of space junk, seen in an illustration. SCIENCE PHOTO LIBRARY/REUTERS

THE ASSOCIATED PRESS

As more space junk comes crashing down, a study shows how earthquake monitors can better track incoming objects by tuning in to their sonic booms.

When a discarded module from a Chinese crew capsule reentered Earth's atmosphere over Southern California in 2024, the sonic booms generated seismic readings. Scientists used those readings to place the object's path nearly 30 kilometers farther south than radar had predicted from orbit.

Using this method to track uncontrolled objects plummeting at supersonic speeds could help recovery teams reach debris more quickly, which is crucial if the debris is dangerous.

"The problem at the moment is we can track stuff very well in space," said lead researcher Benjamin Fernando of Johns Hopkins University in the United States. "But once it gets to the point that it's actually breaking up in the atmosphere, it becomes very difficult to track."

His team's findings, published in January 2026 in the journal Science, focus on a single debris event. But the researchers already have used publicly available data from seismic networks to track a few dozen other reentries.

Scientists and others increasingly worry that space debris could strike a plane in flight.

"There are thousands, tens of thousands, more satellites in orbit than there were 10 years ago," Fernando said. "Unfortunately, we don't really have anything other than the word of the company to say that when they break up, they completely burn up in the atmosphere."

Fernando and his colleagues gathered data from more than 120 seismometers that captured the sonic booms from the Chinese module's reentry, using the data to plot the object's suspected path.

The out-of-control module had been abandoned in a decaying orbit ever since it was cut loose from the Shenzhou-15 capsule returning three Chinese astronauts from their country's space station in 2023. The 1,300-kilogram module broke into countless pieces as it plummeted through the atmosphere, resulting in multiple sonic booms.

The goal is to ascertain, within minutes or even seconds, the speed and direction of incoming space junk as well as its fragmentation. In remote areas such as the South Pacific, nuclear blast monitoring stations could potentially track the sonic booms to fine-tune the paths of descent.

Philippine Coast Guard personnel carry debris from a Chinese rocket that was found in waters off Mamburao, Philippines, in August 2022. PHILIPPINE COAST GUARD/THE ASSOCIATED PRESS

STEPPING UP

Indian forces rehearse for the nation's Republic Day parade in Mumbai in January 2026.

HINDUSTAN TIMES/GETTY IMAGES

RELEVANT. REVEALING. ONLINE.

www.ipdefenseforum.com

Indo-Pacific Defense FORUM is produced for military and security professionals in the Indo-Pacific region.

NEW CONTENT POSTED DAILY!

FORUM ONLINE IS IN 10 LANGUAGES

Chinese (Simplified and Traditional)
English
Hindi
Indonesian
Japanese
Korean
Russian
Thai
Vietnamese

JOIN US ONLINE AND ON SOCIAL MEDIA

SHARE YOUR COMMENTS

ON FORUM'S OFFERINGS AT WWW.IPDEFENSEFORUM.COM

OR EMAIL US AT IPDF@IPDEFENSEFORUM.COM

NOW ON YOUTUBE AND LINKEDIN!

Join us on Facebook, X, Instagram, LinkedIn and YouTube: @IPDefenseFORUM
WhatsApp: @IPDEFENSEFORUM
Line: @330WUYNT

All platforms may not be available at every location.