INDO-PACIFIC DEFENSE

VOLUME 47, ISSUE 3, 2022

FORUM

COMBINED STRENGTH

Strategic Partnerships

features

departments

ABOUT THE COVER:
From left: Gen. Koji Yamazaki, Japanese Chief of the Joint Staff; Gen. Mark A. Milley, chairman of the U.S. Joint Chiefs of Staff; and Gen. Won In Choul, then chairman of the Republic of Korea Joint Chiefs of Staff, team up during a trilateral meeting at Camp Smith, Hawaii, on March 30, 2022.

PETTY OFFICER CARLOS M. VAZQUEZ II/U.S. NAVY

Dear Readers,

Welcome to Indo-Pacific Defense FORUM's issue on strategic partnerships.

Building trust, confidence and cooperation among military and security organizations and governments of allies, partners and like-minded nations is as important for enhancing regional security as is building multilateral capability and interoperability. Russia's invasion of Ukraine and the ensuing war illustrate the role strategic partnerships play not only in defending the homeland but also for preserving regional peace.

This edition shows why creating a thoughtful network of reliable partners is critical for promoting shared values, rules and norms across the region and is important for achieving integrated deterrence in this evolving environment of strategic competition.

In this era, allies and partners must take a fresh look at the adequacy of existing security arrangements to foster capabilities for collective security and defense and to mitigate threats posed by malign actors who are developing advanced technologies, as Dr. Alfred Oehlers, a professor at the Daniel K. Inouye Asia-Pacific Center for Security Studies, explains in his opening article.

The Indo-Pacific's inherited security architecture, which is built upon historic United States alliances with Australia, Japan, the Philippines, South Korea and Thailand, will go a long way in addressing such threats. Nobukatsu Kanehara of Doshisha University also provides a Japanese perspective in this issue on how to improve upon an Indo-Pacific strategy that will maintain peace in the region, including effectively deterring the People's Republic of China from invading Taiwan.

Newer partnership constructs likely will be needed that are tailored to specific technology fields and the requirements of all-domain operations. In another article, retired Indian Army Maj. Gen. S B Asthana recommends a multinational, multidomain response that builds on rising alliance architectures such as the Quadrilateral Security Dialogue that includes Australia, India, Japan and the U.S.

Security outreach already has expanded over the years to include key multilateral organizations and mechanisms. The Association of Southeast Asian Nations (ASEAN) and the ASEAN Defence Ministers' Meeting-Plus stand out as examples, as do engagements with the Pacific Islands Forum and a host of other Indo-Pacific political security arrangements.

The U.S.'s freedom of navigation program will remain a salient tool to counter infringements on the established international order, retired U.S. Navy Capt. Raul Pedrozo, the Howard S. Levie professor on the Law of Armed Conflict at the U.S. Naval War College's Stockton Center for International Law, explains in another piece. The program demonstrates the U.S. commitment to preserving a stable legal system for the world's oceans for all nations, he writes.

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

All the best,
FORUM Staff

IPD FORUM

Strategic Partnerships
Volume 47, Issue 3, 2022

USINDOPACOM LEADERSHIP
JOHN C. AQUILINO
Admiral, USN Commander

STEPHEN D. SKLENKA
Lieutenant General, USMC
Deputy Commander

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

CONTACT US

IPD FORUM

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

ipdefenseforum.com

email:
ipdf@ipdefenseforum.com

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

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

DR. ALFRED OEHLERS joined the Daniel K. Inouye Asia-Pacific Center for Security Studies (DKI-APCSS) in March 2007. Specializing in the political economy of economic growth and development in the Indo-Pacific region, he has taught and written extensively on a range of issues, many connected with the rapid development of East and Southeast Asia, as well as the Pacific islands region. Featured on Page 10

RETIRED INDIAN ARMY MAJ. GEN. S B ASTHANA is chief instructor of the United Service Institution of India, the nation's oldest think tank. A strategy and security analyst, he is a decorated infantry general with 40 years of experience in national and international assignments, including at the United Nations. He has written over 400 articles about strategy and the military. Featured on Page 14

NOBUKATSU KANEHARA is a professor at Doshisha University in Kyoto, Japan. He was assistant chief cabinet secretary to then-Japanese Prime Minister Shinzo Abe from 2012-19. In 2013, he became the inaugural deputy secretary-general of the National Security Secretariat and also served as deputy director of the Cabinet Intelligence and Research Office. His career includes stints in the Ministry of Foreign Affairs as director-general of the Bureau of International Law and deputy director-general of the Foreign Policy Bureau. Featured on Page 20

RETIRED UNITED STATES NAVY CAPT. RAUL PEDROZO is the Howard S. Levie professor on the Law of Armed Conflict at the U.S. Naval War College's Stockton Center for International Law. He served in numerous positions advising senior military and civilian defense officials, including as special assistant to the U.S. undersecretary of defense for policy and senior legal advisor to the commander of U.S. Indo-Pacific Command. He has lectured at myriad academic institutions and written extensively on maritime security and South China Sea issues and is the co-author of several books, including "International Maritime Security Law." Featured on Page 42

RETIRED U.S. NAVY REAR ADM. MICHAEL BAKER has experience in strategy, contingency planning, overseas deployment operations and multinational exercises. He has taught combat casualty care, triage and trauma care, and response to complex disasters and humanitarian emergencies. He has published over 70 peer-reviewed articles and has lectured at numerous international conferences.

JACOB BAKER earned a Master of Professional Studies in the Applied Intelligence Program at Georgetown University School of Continuing Studies. He has co-authored articles on the intersection of intelligence, global health, pandemic surveillance and national security.

DR. DEON CANYON, a professor at DKI-APCSS, specializes in crisis management, biosecurity, the Pacific islands region and gray-zone gaming. His research focuses on understanding, managing, controlling and preventing complex and dynamic security threats with innovative approaches. He has authored hundreds of articles during his 29 years at DKI-APCSS and other U.S. and Australian institutions.

DR. SEBASTIAN KEVANY, a professor at DKI-APCSS, is a specialist in health security, health diplomacy, health as foreign policy, international relations, epidemics, pandemics and global public health. He has also done extensive fieldwork as part of more than 100 missions to Africa, the Middle East and the Pacific island region. Featured on Page 46

Port Partnership

Australia announced in January 2022 that it would provide U.S. $420 million to Pacific neighbor Papua New Guinea to upgrade key ports, amid concern in Washington and Canberra that Beijing's infrastructure investment in the Pacific islands has a military ambition.

Australia's funding will help the Papua New Guinea Ports Corp. increase capacity to accommodate larger ships, including container ships on major trade routes, which will improve trade connectivity, then-Australian Foreign Affairs Minister Marise Payne said in a statement.

The funding will also go toward urgent repairs on coastal wharves that are up to 70 years old. (Pictured: A container ship docks at a port town in Papua New Guinea.)

A Chinese-funded wharf built on another Pacific island, Vanuatu, sparked Australian media reports in 2018 — denied by Vanuatu and Beijing — that the Chinese Communist Party wants to use the facility for military ships. Reuters

CYBER COORDINATION

Australia and the United Kingdom will "fight back" against cyberattacks from Iran, the People's Republic of China and Russia, then-Australian Defence Minister Peter Dutton said.

Australia and the U.K. will coordinate cyber sanctions to increase deterrence, raising the costs for hostile state activity in cyberspace, then-Australian Foreign Affairs Minister Marise Payne said after signing an agreement with U.K. Foreign Secretary Liz Truss in January 2022.

"Australia is committed to working with partners such as the U.K. to challenge malign actors who use technology to undermine freedom and democracy," Payne said in a statement.

Bilateral discussions also identified areas where Australia and the U.K. can work together in the Indo-Pacific region and on Australia's nuclear-powered submarine program. Reuters

Missile Acquisition

The Philippines plans to acquire a shore-based anti-ship missile system from India for almost U.S. $375 million to strengthen its Navy, the Southeast Asian nation's defense minister said.

The Philippines is in the late stages of a five-year, U.S. $5.85 billion project to modernize its military hardware, which includes World War II-era warships and helicopters used by the United States in the 1960s. Under the deal with India, Brahmos Aerospace Private Ltd. will deliver equipment, train operators and maintainers, and provide logistics support, then-Philippine National Defense Secretary Delfin Lorenzana, pictured, said in a Facebook post in January 2022.

The new anti-ship missile system aims to deter foreign vessels from encroaching on the country's 200-nautical-mile exclusive economic zone. In 2018, the Philippines bought Israeli-made Spike extended-range missiles, its first ship-borne missile systems for maritime deterrence.

The Philippines and its allies in 2021 denounced incursions by hundreds of Chinese vessels, described as a maritime militia, into its sovereign territory in the West Philippine Sea.

Reuters

STRONGER TOGETHER

France and Japan face shared security challenges in the Indo-Pacific that are only "getting tougher," Japan's then defense minister said ahead of talks between the foreign and defense ministers of the two countries in early 2022.

The talks between Tokyo and Paris took place as Japan pushed to bolster security cooperation with Western allies as it faces the People's Republic of China's growing assertiveness and North Korea's missile development.

France has overseas territories in the Indo-Pacific and stations its Armed Forces in the region. Rising tensions relating to democratic Taiwan, over which the Chinese Communist Party asserts sovereignty, have put a sharp focus on Japan's security role. North Korea's rapid sequence of weapons tests in January 2022 caused additional concerns.

"Unilateral attempts to change the status quo with force are continuing in the Indo-Pacific region, and the security environment surrounding Japan and France is getting tougher and unstable," then-Japanese Defense Minister Nobuo Kishi said. Kishi and Japanese Foreign Minister Yoshimasa Hayashi met with their French counterparts, then-Foreign Minister Jean-Yves Le Drian and then-Armed Forces Minister Florence Parly, via video conference, pictured.

In a statement, the countries said they agreed to strengthen security cooperation and increase bilateral cooperation in the Indo-Pacific. "The four ministers shared serious concerns about the South and East China Seas situation and agreed to strongly object to unilateral attempts to change the status quo with force," the statement said. "They also confirmed the importance of peace and stability in the Taiwan Strait and agreed to urge relevant parties to solve the cross-strait issue peacefully."

Japan and France have reached several key security deals, including an agreement on the transfer of defense equipment and technology, and have also increased joint military drills in recent years. Reuters

INDO-PACIFIC TERROR THREAT

Indonesian Navy commandos conduct an anti-terror drill in Bandar Lampung.

Singapore Think Tank Reveals Decline in 2021

BENARNEWS
PHOTOS BY AFP/GETTY IMAGES

Terrorist threats in Southeast and South Asian countries declined in 2021, a Singapore think tank said in its annual threat assessment published in January 2022, noting that COVID-19 movement restrictions had "flattened the curve of terrorism."

There were fewer terror-related incidents in Bangladesh, Indonesia, Malaysia and the Philippines as governments battled the pandemic, according to the "Counter Terrorist Trends and Analyses" report published by the S. Rajaratnam School of International Studies.

In Thailand in 2021, meanwhile, violent incidents connected to an insurgency in the far south were similar to those in 2020, researchers found.

"Ultimately, the 2021 survey underscored the continuing imperative for states to address the longer-term underlying grievances that fuel violent extremism," the analyses said.

In Indonesia, Southeast Asia's largest country, the number of attacks and plots by extremist Islamic militant groups dipped during the two years spanning 2020 and 2021 compared with before the outbreak of COVID-19, according to the report. Jamaah Ansharut Daulah's (JAD's) relatively stagnant activities in 2020-21 and the decline of East Indonesia Mujahideen's (MIT's) terror activities in 2021 "can be partly attributed to movement restrictions and higher costs associated with domestic travels due to the pandemic," the report said.

In 2021, JAD was involved in at least nine incidents, including five using explosive materials. Those included two suicide bomb attacks and a suicide bomb plot, compared with 11 incidents the previous year.

Police were terrorists' most common target in Indonesia, the analyses found. Others targeted by Indonesian extremists in 2021 were "civilians, including Christians, as well as both Indonesian and mainland Chinese," the report said.

In early January 2022, Indonesian security forces announced they had killed Ahmad Gazali, a suspected MIT member, in the mountains of Central Sulawesi province, cutting MIT's membership down to only three.

Philippine Marines conduct counterterrorism training as part of a partnership with the Australian Defence Force.

Indonesian Navy commandos participate in anti-terror training in Bandar Lampung, Indonesia, in September 2021.

Malaysia, the Philippines

The analyses specifically linked the pandemic and the drop in terror activities in Malaysia in 2021. "The pandemic-driven movement restrictions that hampered inter-state and international movements also 'flattened the curve of terrorism' in Malaysia."

Authorities made no terror-related arrests in Peninsular Malaysia in 2021, but they made about 15 in the Malaysian state of Sabah on the island of Borneo between May and September 2021. There were seven arrests in 2020, 72 in 2019, 85 in 2018, 106 in 2017 and 119 in 2016, the analyses found.

Still, the analyses expressed concern that terror threats had moved online.

"The government-imposed lockdowns have forced people to spend more time online, raising the likelihood of vulnerable individuals being exposed to radical ideologies in the cyber domain. Around the region, groups such as IS [Islamic State] have increased their recruitment and radicalization efforts through social media during the pandemic," it said.

Elsewhere, the Armed Forces of the Philippines drew praise for capturing terror bases in the southern region of Mindanao. Nationwide, the number of successful terrorist incidents dropped from 134 in 2019 to 59 in 2020 and 17 in 2021, the analysts said, defining a successful incident as an attack that injured or killed others.

The analyses noted that government-imposed COVID-19 lockdowns affected terror operations. "Given they significantly limited the movements of the general population, as well as those of terrorists, this has rendered terrorist logistics vulnerable to being detected more readily," it said.

Bangladesh, Thailand

In Bangladesh in 2021, "there were two failed attacks compared to four successful ones in 2020," the report said, adding that authorities arrested about 130 terrorist suspects nationwide.

Neo-JMB, a pro-IS breakaway faction of Jamaat-ul-Mujahideen Bangladesh, "appeared to target law enforcement agencies, churches, noted Hindu and Buddhist personalities and workers of non-governmental organizations," the analyses said.

It also said that Neo-JMB sought to train its members how to produce improvised explosive devices, as well as "chloroform bombs to target buses, classrooms and public places in its bid to kill silently."

In Thailand's insurgency-hit southern border region, 423 violent incidents were recorded, with 104 people killed and 169 injured, through November 2021, according to the report. The scale was similar to 2020 when 335 violent incidents occurred, killing 116 and injuring 161.

In the Muslim-majority Deep South, as the region is known, more than 7,000 people have been killed since separatist groups resumed an insurgency against the Buddhist majority 18 years ago.

The Barisan Revolusi Nasional (BRN), the Deep South's largest separatist group, scaled down its militant operations on humanitarian grounds in April 2020 because of the pandemic. The analyses said this led to a "significant decline in violence."

"In 2021, the BRN maintained low-level operations, so as not to aggravate the already perilous situation for southern residents," it said.

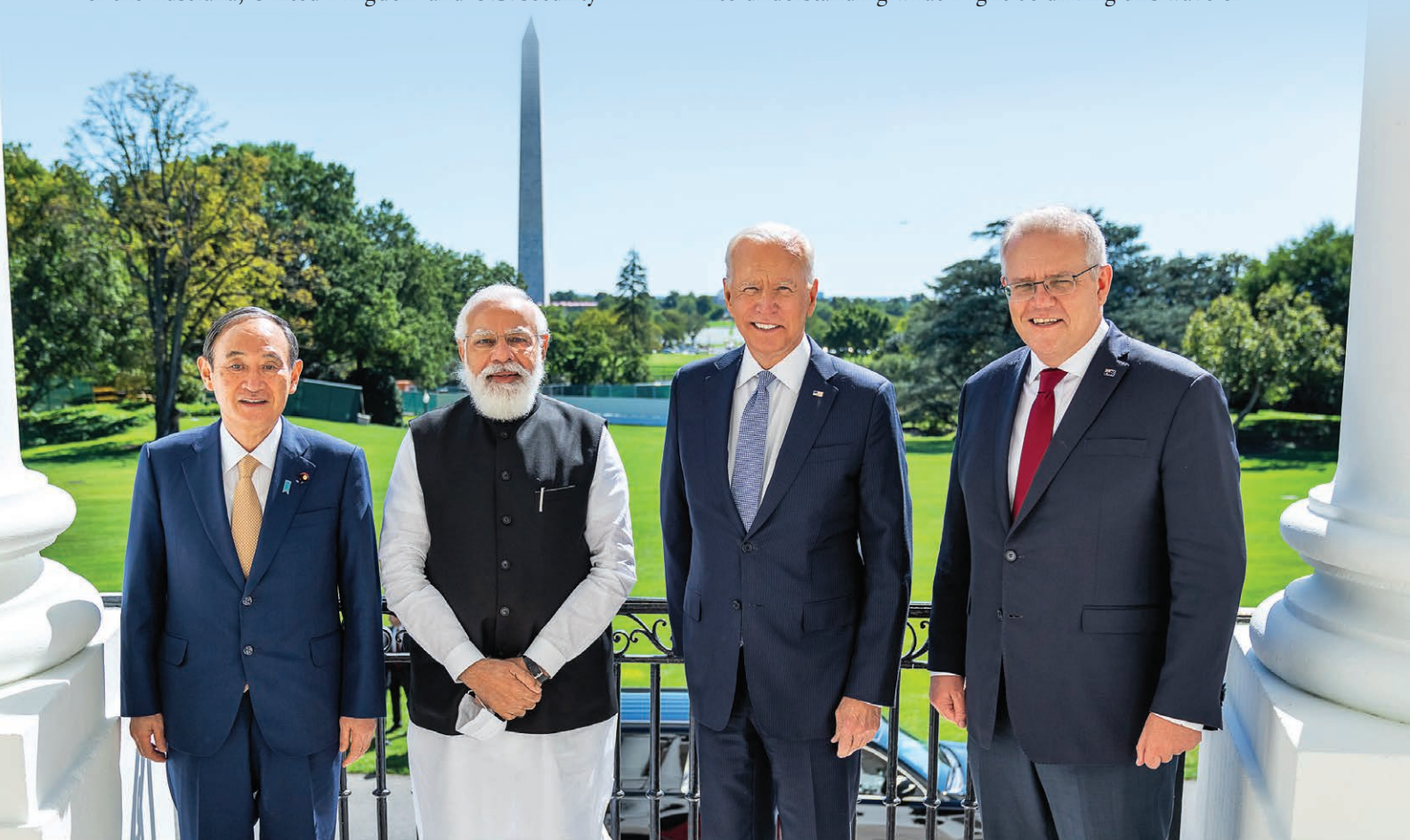
After avoiding peace talks with government officials, in early 2020, BRN rejoined the efforts brokered by Malaysia. A government source said the two sides met virtually in 2021 and the BRN submitted a cease-fire proposal in May 2021, according to the analyses.

RISING Relationships

Understanding the New Era of Indo-Pacific Alliances and Partnerships

DR. ALFRED OEHLERS
DANIEL K. INOUYE ASIA-PACIFIC CENTER FOR SECURITY STUDIES

The past year saw much media coverage of newer strategic partnerships in the Indo-Pacific. The Quadrilateral Security Dialogue, or Quad — whose members are Australia, India, Japan and the United States — continued to figure prominently, with September 2021 witnessing further maturation of this forum with the first Quad Leaders' Summit in Washington, D.C. Underscoring the innovative tilt in security arrangements was the announcement of the Australia, United Kingdom and U.S. security partnership, known as AUKUS, earlier that same month. Analysts described AUKUS, which will deepen defense science, technology and industry integration among the partners, as a harbinger of many similar trilateral or mini-lateral pacts to come. Commentators quickly seized on this, highlighting the uptick in security arrangements as the dawn of a new era of alliances and partnerships in the Indo-Pacific. Whether this will be the case remains to be seen. For now, it may be instructive to delve deeper into understanding what might be driving this wave of



reconfigurations in strategic relationships by the U.S. and like-minded partners in the region.

There already exists a rich tapestry of alliances, partnerships and relationships in the Indo-Pacific developed by the U.S. and partners since the end of World War II. This overarching architecture has enabled the navigation of successive geopolitical and security challenges and the establishment of an international rules-based order providing decades of stability, security and prosperity for much of the Indo-Pacific. The U.S. alliances with Australia, Japan, the Philippines, South Korea and Thailand are widely seen as cornerstones of this architecture. But these alliances are nested in a wider, dense network of bilateral security relations that enmesh nearly every nation in the Indo-Pacific. Underpinned by robust civil and military diplomacy and extensive security assistance and cooperation programs, such outreach has expanded over the years to include key regional multilateral organizations and mechanisms. The Association of Southeast Asian Nations (ASEAN) and the ASEAN Defense Ministers Meeting-Plus are noteworthy examples, as are engagements with the Pacific Islands Forum and a range of other Indo-Pacific political-security arrangements, often with a specialized service or functional focus.

Leaders from Quadrilateral Security Dialogue nations discuss ways to advance regional cooperation at the group's first in-person summit in September 2021 at the White House in Washington, D.C. THE ASSOCIATED PRESS

If these arrangements have served well in the past, why the impulse toward reconfigurations? Quite simply because times have changed. The post-WWII security architecture largely developed in a different context, addressing different conditions and circumstances. The security solutions the architecture was designed to facilitate related initially to the challenges of the Cold War and confrontation with the Soviet Union. The eventual disintegration of the Soviet Union and end of the Cold War saw a short interval of "drift" in the U.S., which was soon replaced by a focus on the war on terror and security capacity and institution building to address extremist challenges to state stability. Reflecting this trajectory, much of the thinking around security architecture engagement and development until recently has drawn on some amalgam of themes associated with countering extremism and terrorism, security or defense capacity development and institutional enhancement, or more ambitious nation building.

From left: Then-Japanese Prime Minister Yoshihide Suga, Indian Prime Minister Narendra Modi, U.S. President Joe Biden and then-Australian Prime Minister Scott Morrison participate in the Quadrilateral Security Dialogue summit. REUTERS

DECEPTIVE COMPARISONS

The current context is a dramatic departure from this past, defined by the rapid emergence of the People's Republic of China (PRC) as a pacing competitor to the U.S. and a force undermining the international rules-based system and sovereignty of partners in the Indo-Pacific. Although on the surface the challenges posed by the PRC might invite comparison with the Soviet era, this can be deceptive. The PRC represents a different entity than the Soviet Union, making the task of addressing it much more complex. Far from being independent, it has immersed itself in the international political and economic system and turned this to its advantage. Leveraging all elements of national power in state-led programs such as the One Belt, One Road infrastructure scheme, the PRC has subverted, cajoled and coerced nations of lesser means. Meanwhile, through a panoply of insidious gray-zone tactics just short of the threshold of war, it has strengthened its hand without triggering conventional security responses capable of inflicting punishing costs. These challenges are neither comparable to Cold War confrontation nor soluble in the same ways that allies countered terrorism and built partner nation security capacities. How we have configured alliances and partnerships needs to be revisited while new configurations are explored to better meet current challenges.

The relentless march of technology makes this reconfiguration more crucial. Tech-enabled domains such as cyber and space are now pivotal for national security and strategic competition. When fused with advanced capabilities in artificial intelligence, quantum computing and 5G or 6G telecommunications, the prospects for highly sophisticated multidomain operations are increasingly feasible. Yet, such technologies and capabilities were hardly imaginable when the foundations of much of the Indo-Pacific alliance and partnership architecture were evolving during the second half of the 20th century. It is imperative to reassess the adequacy of our security partnerships and arrangements to not

U.S. Secretary of State Antony Blinken, left, and Indonesian Foreign Minister Retno Marsudi participate in a meeting of Association of Southeast Asian Nations foreign ministers in September 2021 on the sidelines of the United Nations General Assembly in New York. THE ASSOCIATED PRESS

only foster such readily accessible capabilities for the collective security and defense of like-minded partners but also to head off the threat they pose when developed and deployed by malign actors. Updating an inherited architecture may get us partway in this effort. Likely, newer partnership constructs will be needed that are unique to these technology fields and the requirements of all-domain operations.

GRAY ZONES

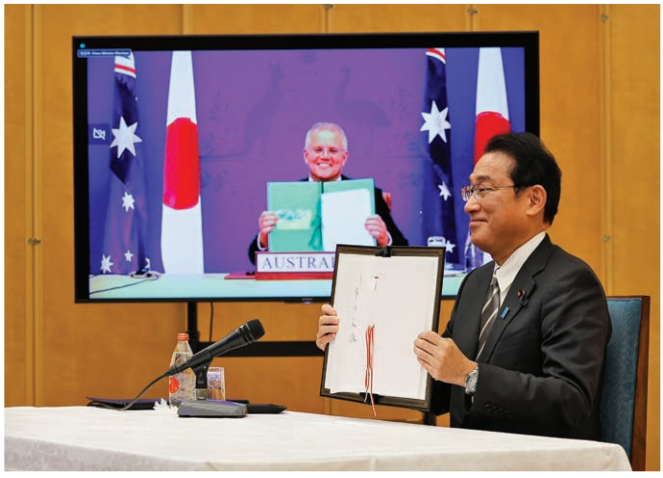
Today, the Indo-Pacific faces an expanded threat spectrum that challenges the relevance and effectiveness of our alliances and partnerships. Involving diverse elements of state power — and with the private sector and even nongovernmental and criminal groups dragooned into service — the PRC's gray-zone tactics and multidimensional threats typically bring to bear much more than military force on any matter of consequence. Increasingly, it is rare that anything is purely a security or defense issue, especially when political, diplomatic, legal, economic, financial, technological and information considerations are added to the mix to convolute and confound. Yet, we remain wedded to alliances and partnerships that historically rest on pristine and narrowly conceived notions of security or defense. No matter how exquisite this partnership architecture might be, it risks paralysis in the face of ambiguous situations where no definitive "smoking gun" can be identified to trigger mutual defense or security obligations. How many incursions by maritime militias amount to an act of war? How many state officials or political representatives need to be corrupted and influenced before a national security threat is recognized, invoking treaty provisions? To counter the prospect of such paralysis, it is timely to reframe the nature and scope of such partnerships to reflect the subtleties of the strategic competition being waged, where things are often won or lost without a shot being fired. Updating the old and finding new, more effective partner configurations is essential.

It is timely to reframe the nature and scope of such partnerships to reflect the subtleties of the strategic competition being waged, where things are often won or lost without a shot being fired.

Issues of strategic competition aside, the 21st century has already shown a future likely to be characterized by threats of a severity, magnitude and complexity that outstrip the capacities of existing multilateral cooperative mechanisms. The enduring COVID-19 pandemic is a case in point, but so, too, is the challenge of climate change. Each has greatly exacerbated insecurities in the Indo-Pacific and will continue to do so for years to come. They both have also severely tested international cooperative mechanisms, prompting urgent efforts to develop options for dealing

U.S. President Joe Biden attends the U.S.-Association of Southeast Asian Nations virtual summit from the White House in October 2021.

THE ASSOCIATED PRESS



Japanese Prime Minister Fumio Kishida, right, and then-Australian Prime Minister Scott Morrison display their nations' Reciprocal Access Agreement during a virtual summit in January 2022.

THE ASSOCIATED PRESS

with priorities. COVID-19, for example, prompted arrangements of varying scale and scope to address issues such as personal protective equipment shortages, and vaccine research, development and distribution. Related to climate change, innovative partnerships continue to emerge to serve urgent priorities in humanitarian assistance and disaster relief. They will likely expand to strengthening resilience in partners and exploring scientific, technological and organizational solutions. Alongside mature alliances and partnerships, cooperative arrangements unique to these and other crises will likely develop, sometimes of an ad hoc nature with specific objectives and priorities and varying life spans.

PARTNERSHIPS MATTER MORE NOW

Partnerships have always mattered. However, owing to the security solutions needed now — and in the future — some aspects of partnership development are likely to have more exacting requirements and expectations. As the example of AUKUS suggests, a qualitatively deeper level of commitment and integration is required to decisively address challenges with agility, speed and impact. By necessity, some future partnerships may be more selective and tailored, bringing together a narrower range of partners with closely aligned interests and complementarities. This may cause apprehension. Proponents of regional and subregional multilateralism, for example, may fear a dilution of commitment. Such alarm is misplaced. There will always be a place for inclusive and representative pan-regional or subregional arrangements, and the commitment to these is unlikely to diminish. That said, there must also be an increasing scope for smaller arrangements that allow groups of nations to move with speed and agility to solve urgent challenges or needs. Offering an additional dimension, such mini-laterals need not detract from or undermine the alliance and partnership architecture. In fact, they have the potential to strengthen the overall architecture to better fulfill the aspirations of regional peace, security and prosperity.

In a commentary on AUKUS for Defense News in December 2021, then-Australian Minister for Defence Industry Melissa Price singled out Australia's rapidly deteriorating strategic environment as a major factor behind the pact. Most Indo-Pacific nations may share such pessimistic strategic assessments. Allies, partners and like-minded countries would be remiss if they did not take stock of their readiness to face this troubling context. A robust reassessment of the adequacy of alliance and partnership arrangements must be a high priority. Given the strategic competition, the question must be: "Is what we have now in our alliances and partnerships enough?" Likely, the answer will be: "We have to do more." □

A UNIFIED Multidomain Solution

The Chinese Communist Party's threat to the Indo-Pacific region requires a multinational, multidimensional response

INDIAN ARMY MAJ. GEN. (RET.) S B ASTHANA

An activist protests outside the Chinese consulate in Makati, the Philippines, after a Chinese coast guard vessel fired water cannons at Philippine supply boats near a disputed shoal in the South China Sea in November 2021. THE ASSOCIATED PRESS

During a conversation with United States President Joe Biden, Chinese Communist Party (CCP) General Secretary Xi Jinping attempted to create the impression that a bipolar world order exists. Xi's aggressive posturing during that November 2021 virtual summit was likely rejuvenated by his unchallenged mandate in the sixth plenary session of the CCP's 19th Central Committee, despite that nations worldwide continue to rebalance among unipolar, bipolar and multipolar global orders, depending on their varying perceptions.

Unless the global community generates a realistic response across all domains — land, sea, air, space and cyberspace — Beijing will use all of its instruments of power — ethically and unethically — including exploiting the COVID-19 pandemic to become the sole superpower on the global stage and to establish a China-centric Indo-Pacific region.

Defining the Multidimensional Threat of China

The People's Republic of China (PRC) has employed a strategy to incrementally encroach on the sovereign territory of other nations. This extension of the CCP's "active defense" strategy, released in a 2015 white paper that called for a greater Chinese naval presence farther from the PRC's shores, has led to the creation of artificial maritime features converted into military bases in the Indo-Pacific, proving that previous freedom of navigation operations and naval posturing by other nations were not adequate to deter the CCP from disturbing the rules-based order. The PRC has incrementally extended its sovereignty claims based on its one-sided interpretation of history in the South and East China seas and Taiwan, among other territories. A similar encroachment in India's Ladakh region proved that the PRC will violate any signed agreement or treaty with other nations if the CCP requires.

When an international tribunal declared the PRC's nine-dash line claims legally invalid in its territorial dispute in the South China Sea with the Philippines, the CCP ignored the ruling. The CCP showed that any verdict by any international institution that doesn't suit the party's strategic interests will be scrapped. With the expansion of its so-called comprehensive national power, the CCP started strengthening its military in all domains of warfare. It has already developed its navy to become the largest in the world in terms of fleet size. It has also taken steps, such as passing its China-centric Coast Guard Law in 2018 and its amended Maritime Traffic Safety Law in 2016, to challenge the international order by threatening the use of the global commons and the exclusive economic zones of countries with overlapping claims and access to one of the busiest global sea lines of communication (SLOC) in the Indo-Pacific.

In developing its multidomain warfare capabilities, the CCP has made rapid strides in space warfare in terms of assets and disruptive technology. The CCP has also boosted its conventional capabilities and plans to expand its nuclear arsenal to about 1,000 warheads by 2030. The list of the CCP's force multipliers seems dangerously

impressive with the application of artificial intelligence, quantum computing, long-range vectors, hypersonic systems and cyber capabilities. Although the quality of the CCP's military hardware, which has historically been suspect, was achieved largely as a result of pirated technology or reverse engineering, it's adequate to deter some potential adversaries and achieve the CCP's longtime objective of "winning without fighting."

The most concerning aspect of China's capacity building is in the sphere of nonkinetic warfare capabilities, which entail the application of military capabilities in a cohesive manner while ensuring minimum physical contact of forces. Chinese economic, technological and digital offensives against other countries have rendered those nations increasingly dependent on China, eroding their independence and muting their responses to the CCP's unethical overreach. With investments from the West, the PRC became a global manufacturer and supplier, gaining supply chain dependencies to an extent that the responses by individual countries will remain muted unless alternative resilient supply chain and manufacturing hubs are established. The PRC's economic encroachment is mixed with an economic offensive on countries that don't toe the CCP's line, such as Australia. The CCP's digital offensive is even more targeted, and its biological warfare capabilities have already shaken the world.

The PRC has nearly 30 outposts in the Paracel and Spratly islands in the South China Sea, including Fiery Cross Reef, pictured. Since 2013, the PRC has built 1,200 hectares of artificial islands featuring military and other facilities. ASIA MARITIME TRANSPARENCY INITIATIVE

The CCP's strategic use of the "three warfares" — namely media or public opinion, psychological and legal — is evidenced in its exhibition of newly acquired combat capabilities in terms of military hardware, technology, exercises and buying opinions. Its three warfares tactics appear to be gaining ground in election-oriented segments in politically active democracies.

Chinese Vulnerabilities

The challenge presented by China is significant but not insurmountable because it has major vulnerabilities. Its long SLOC that passes through various chokepoints in the Indo-Pacific is a vulnerability. The PRC has sought to mitigate its risks through connectivity projects, such as the China-Pakistan Economic Corridor, the China-Myanmar Economic Corridor and its overall strategy to develop a network of Chinese military and commercial facilities, including ports and airfields, that extend from the Chinese mainland across Southeast Asia to the Horn of Africa, and develop diplomatic relations with the host countries to ensure its energy supply. The nodes of the necklace connect mainland China to the Arabian Sea and Persian Gulf via the South China Sea, the Malacca Strait and the Indian Ocean. Lately, the PRC seems to be seeking to extend the chain to Africa and Central Asia. Yet all the nodes potentially could be exploited.

Cracks are emerging in the Chinese economy after the failure of many One Belt, One Road (OBOR) infrastructure investment projects, the bursting of the real state economic bubble and the CCP's cleansing, or "common prosperity," drive to redistribute wealth that shook up capitalists and investors. The CCP's attempts to crush dissent in regions such as Xinjiang, Tibet and Hong Kong also reveal its fear of losing control, evident in its domestic surveillance budget and use of techniques such as profiling. To quell dissent, the CCP spends more on internal security than on national defense. China's economy and its SLOC are the center of gravity in tackling the challenges posed by the PRC because China's people will continue to tolerate Xi's autocratic regime as long as it keeps delivering economically. Without economic successes, however, China has few friends internally or externally. Targeting human rights abuses may cause the CCP leadership discomfort, but the issue falls short of a strategic vulnerability at least for now.

Continued on Page 18

China's One Belt, One Road Maritime Trade Route

A Network of Chinese-Controlled Ports That Encircle India and Connect Mainland China to Africa and Europe

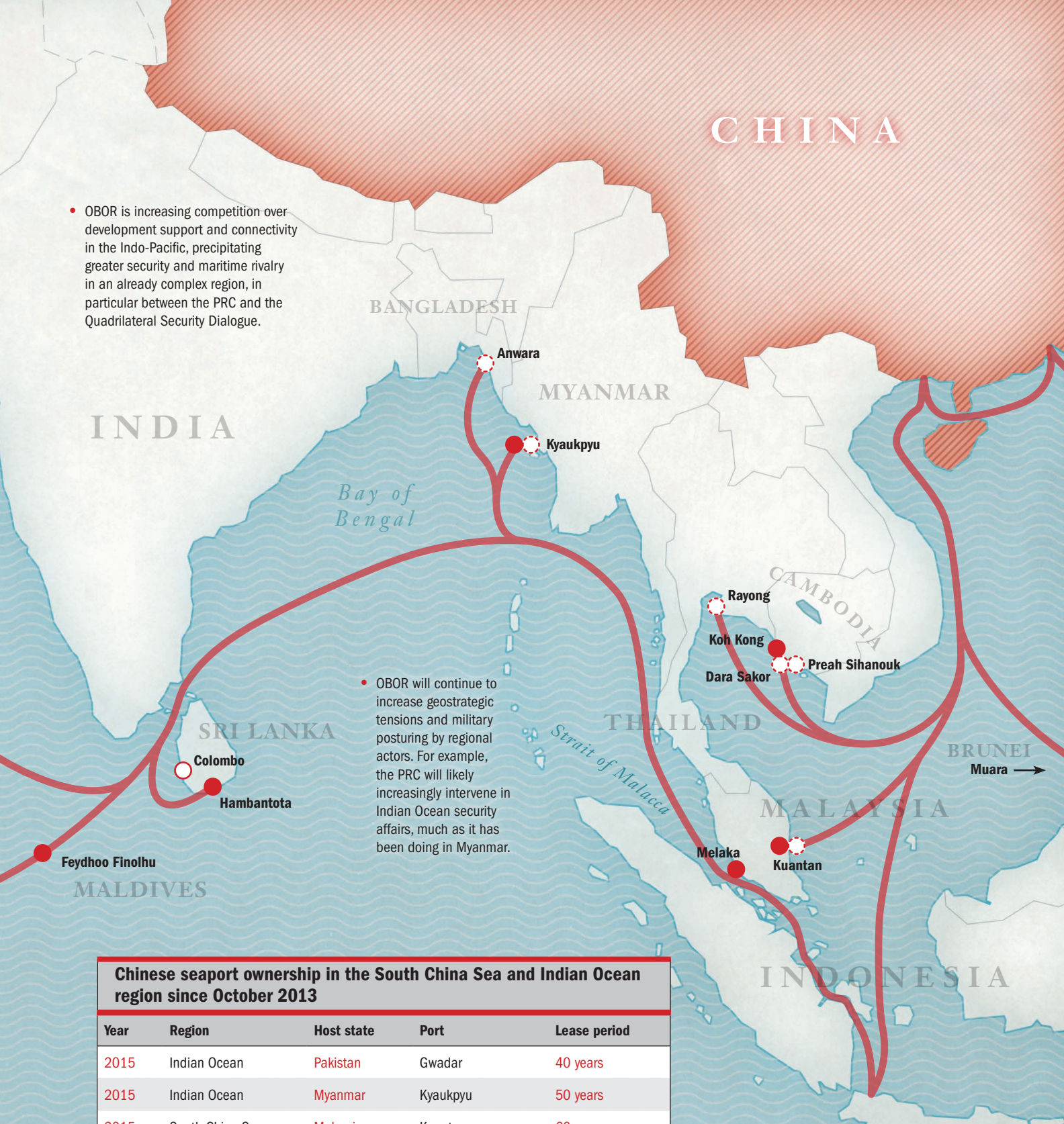
- The People's Republic of China's (PRC's) One Belt, One Road (OBOR) infrastructure plan entails a trade network linking the Chinese mainland across Southeast Asia and the Indian Ocean region to the Horn of Africa. Along with the maritime routes, the PRC intends to build land routes to shore up vulnerabilities in its port network via a hub-and-spoke scheme of highways.

Aircraft carriers and other warships from members of the Quadrilateral Security Dialogue — Australia, India, Japan and the United States — participate in the Malabar exercise in the northern Arabian Sea.

INDIAN NAVY/THE ASSOCIATED PRESS

- The PRC's vast infrastructure scheme presents vulnerabilities along its sea lines of communication. To enhance its control, the PRC seeks to build a military presence at many of the route's commercial ports.

- OBOR could reshape the nature of the Indian Ocean trade route, now an interconnected global commons, and its security architecture. OBOR is exacerbating tensions between the PRC and regional states over the PRC's strategic intentions, a regional arms buildup and territorial disputes, especially in the South China Sea.



Chinese seaport ownership in the South China Sea and Indian Ocean region since October 2013

Year	Region	Host state	Port	Lease period
2015	Indian Ocean	Pakistan	Gwadar	40 years
2015	Indian Ocean	Myanmar	Kyaukpyu	50 years
2015	South China Sea	Malaysia	Kuantan	60 years
2016	Indian Ocean	Djibouti	Obock	10 years
2016	South China Sea	Malaysia	Melaka	99 years
2017	Indian Ocean	Sri Lanka	Hambantota	99 years
2017	South China Sea	Brunei	Muara	60 years
2017	Indian Ocean	Maldives	Feydhoo Finolhu	50 years

Note: Transparency issues mean that data on the year of agreement and lease period may be inaccurate.
Source: Data compiled by Richard Ghiasy, Fei Su and Lora Saalman for the Stockholm International Peace Research Institute.

FORUM ILLUSTRATION

European Union Commission President Ursula von der Leyen, left, and European Commissioner for International Partnerships Jutta Urpilainen discuss the U.S. $340 billion Global Gateway infrastructure investment program in Brussels in December 2021.

REUTERS

Continued from Page 15

Why Democracies Need to Unite

China has been trying to sell the narrative that its system of governance is better than democracy based on its claims that it has fared better during the COVID-19 pandemic in terms of public health outcomes and economic recovery. The PRC's OBOR scheme, while increasing China's strategic footprint globally, has pushed many needy countries into its unsustainable debt structures and restricted their sovereign choices in the absence of better financing alternatives, notwithstanding the many problems with OBOR projects. To impose the CCP's concept of "unrestricted warfare," the PRC is seizing real estate, exploiting host countries' critical mineral resources such as rare earth minerals, installing dual-use bases worldwide for potential military purposes and manipulating the global financial system. The CCP is also increasingly confident that democracies won't be able to come together on many issues because they often have dissenting views and groups that are easy to exploit. The China challenge has become big enough for a collective response by like-minded democracies.

A Multinational, Multidimensional Response

The Indo-Pacific is the economic, trade and population hub of the future, with the largest markets, some of the busiest SLOCs and vast natural resource potential. All of the world's powers seem to be gravitating toward the region, which also possesses some of the most dangerous flashpoints, such as the Korean Peninsula, the South and East China seas, and Taiwan. It also is where Chinese influence is approaching a maximum. To take on the Chinese challenge, regional partners along with like-minded democracies need to synergize their actions, as

Leaders of like-minded nations attend the Group of Seven foreign ministers meeting in Liverpool, United Kingdom, in December 2021.

REUTERS

Xi tries to force the nine-dash line on members of the Association of Southeast Asian Nations (ASEAN) and the CCP becomes increasingly emboldened to alter the global balance. The United Nations can do little to stymie the PRC, given its veto power as a U.N. Security Council permanent member and its growing clout in other U.N. organizations. Other multilateral, issue-based organizations will be required to deal with segments of the CCP's multidimensional threat, including kinetic and nonkinetic warfare elements.

Expanding Security Partnerships

Notwithstanding the Chinese threat, a direct military confrontation is cost-prohibitive for all, given the destructive potential possessed by major world powers. As a result, bilateral and multilateral groupings assume even greater significance, among them: the Quadrilateral Security Dialogue, or Quad, which includes Australia, India, Japan and the U.S.; the new security alliance of Australia, the United Kingdom and the U.S., known as AUKUS; the Five Eyes (FVEY) alliance of intelligence agencies from Australia, Canada, New Zealand, the U.K. and the U.S.; and NATO.

Countering Chinese maritime threats requires collective action by like-minded democracies, strategic partners and allies to create a multifront approach that can threaten the PRC's SLOC at various chokepoints and draw the People's Liberation Army Navy (PLAN) as far from China's eastern seaboard as possible. That would overextend the PLAN as it sought to protect the SLOC, thus creating vulnerabilities along its network of Chinese military and commercial facilities across Southeast Asia, which could be blockaded.

The Quad's March 2021 statement calling for a free, open, inclusive and healthy Indo-Pacific "anchored by democratic ideals and unrestrained by coercion" presented the CCP with a fundamental challenge to its dream of a China-centric region. The Quad's highlighting of freedom of navigation and overflight did not go unnoticed — the CCP is fully aware that it is being referred to as a threat to a Free and Open Indo-Pacific.

Although a nonmilitary grouping, the Quad has shared security challenges to address, including in cyber, space, critical technology, counterterrorism, infrastructure and health security. The Quad members, for example, are collaborating to provide 1 billion COVID-19 vaccines globally.

India's location makes it crucial to the global response to the challenge of the PRC, on the continent and in the maritime domain. India is in a long-running standoff with China over their shared border and also dominates the most vulnerable segment of China's SLOC in the Indian Ocean. The military capacity building of India is important for a strong response to China across all domains; therefore, strategic partners need to collaborate in developing India's military capacity.

Through AUKUS, Australia eventually will acquire nuclear-powered submarines, which will help blunt Chinese expansionism in the Indo-Pacific. Similarly, efforts by the U.S. and other Quad Plus members to collaborate with global stakeholders, including ASEAN members facing Chinese coercion, are a positive step. Beijing cannot miss the message: Military interoperability among like-minded nations will prove a powerful deterrent should Chinese aggression cross the threshold of global tolerance.

There also is a need to establish alternative supply chains and trade and technology ecosystems that are independent of China, such as initiatives launched by the Quad. These can be supplemented by economic partnerships such as the Build Back Better World involving the Group of Seven industrial nations and other cooperative efforts to counter China's OBOR scheme, such as the Blue Dot Network established by Australia, Japan and the U.S., and the European Union's Global Gateway program, valued at U.S. $340 billion.

Cyber, space, artificial intelligence, hypersonic weapons, quantum technologies, undersea capabilities, biological threats and nuclear expansion require a coordinated global response, with technological development and sharing. The Quad has the potential to become one of the most effective tools for resisting Chinese adventurism. Expanding the Quad Plus with a formalized structure, meanwhile, will be critical for dealing with the challenges posed by an aggressive China. □

Indian Prime Minister Narendra Modi participates in the Leaders' Summit of the Quadrilateral Security Dialogue with Australia, Japan and the United States at the White House in Washington, D.C., in September 2021. REUTERS

FORUM ILLUSTRATION

A Japanese perspective on how to implement an Indo-Pacific strategy

NOBUKATSU KANEHARA/DOSHISHA UNIVERSITY

PHOTOS BY THE ASSOCIATED PRESS

Today, a liberal international order in the Indo-Pacific is emerging for the first time in modern history. Most people in this region came through different paths than those followed by most Westerners and Japanese. Many Indo-Pacific countries were colonized, and their people were racially discriminated against. After World War II, these nations proudly declared independence, but some had to fight for their freedom and suffered tremendous casualties. Immediately after achieving independence, they did not necessarily cherish the Western style of democracy because the colonial powers were mainly democracies, with the exception of Russia, which turned into a communist dictatorship. The liberated countries and territories explored types of dictatorship, including the communist variety tried in Vietnam; the military dictatorships tried by Indonesia, Myanmar, South Korea and Taiwan; and the populist dictatorship tried in the Philippines. Although the regimes were oppressive, some achieved spectacular economic development. In the 1980s, just before the end of the Cold War, some of these Indo-Pacific nations turned one by one to democracy and are now proud members of the club of freedom.

The region embraces 60% of the world's population and soon will account for 60% of the global gross domestic product (GDP). This is an inevitable and historical necessity. The Industrial Revolution that began in Great Britain has changed the world forever. The harbingers of this economic change are today called advanced industrial democracies. Now the wave of industrialization has hit the shores of the Asian continent. China and India, given their size and might, are exerting influence on world politics and the world economy. China, which benefited most from the open and liberal international system, became the second-biggest economy on Earth. Unfortunately, the People's Republic of China (PRC) now stands as a challenger to the liberal international order and wants to carve out its own sphere of interests. The Chinese Communist Party (CCP) seems determined to survive as a dictatorship and dominate the Indo-Pacific.

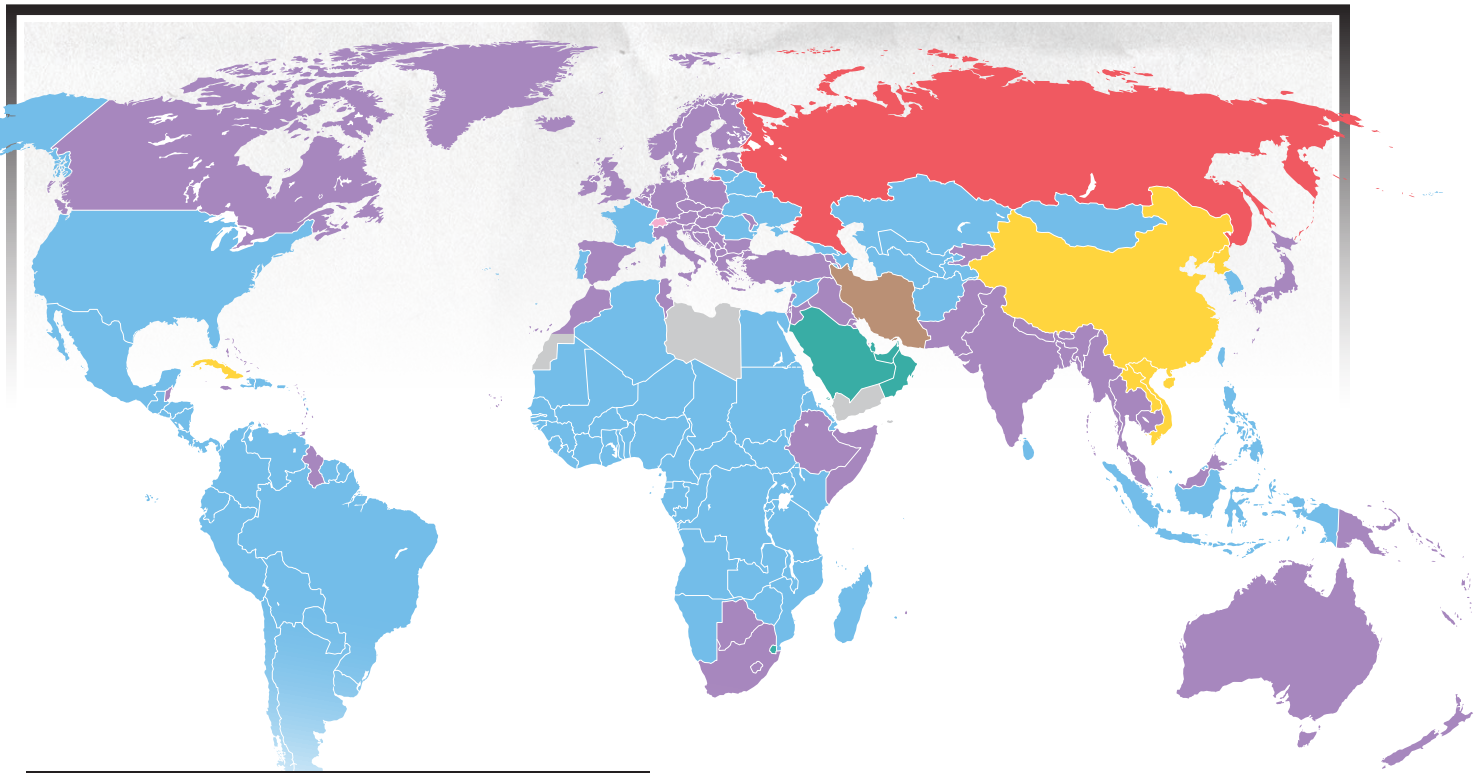
The West faces the CCP's challenge. The region is approaching a watershed moment that will determine whether the West expands its liberal order in the Indo-Pacific or surrenders the whole of the Indo-Pacific to Chinese dominance.

Fumio Kishida, Japan's prime minister, attends a news conference in Tokyo in October 2021 before talks with U.S. President Joe Biden on strengthening the nations' security alliance and regional security cooperation.

How the PRC Emerged

After Japan was defeated in the Pacific War in 1945, the United States curtailed its cooperation with a then-corrupt Kuomintang, also known as the Chinese Nationalist Party. Joseph Stalin, the communist dictator of the Soviet Union, rapidly increased help to Mao Zedong, the leader of the CCP, to conquer China. A brief honeymoon between the Soviet Union and China started. Mao established the PRC in 1949. It was born from the gun by an arm of the party for the communist revolution. Human dignity, conscience, freedom and religion were all denied for the sake of the revolution.

TYPES OF GOVERNMENTS AROUND THE WORLD



Sources: Government GeoInquiries, Esri | Maps.com, Natural Earth, CIA World Factbook, CIA, Freedom House, National Constitution Center (as of 2018)

Mao's attempt to transform the Chinese economy from agrarian to industrial in the 1950s through his Great Leap Forward plan failed dramatically, as tens of millions of people starved to death. Mao was criticized by some party leaders for his lack of leadership during the Great Leap Forward. To solidify his position and eliminate any rivals, he then started the Cultural Revolution. This movement incited youngsters known as the Red Guards to eliminate potential rivals and any ideas contrary to the notion of Mao controling the CCP. From the chaos, Mao retained control and practically turned his rule into a personal cult.

After Stalin's death in 1953, Nikita Khrushchev became leader of the Soviet Union and initiated a thaw with the West. A power-driven Mao started to move away from Russia. In 1969, he started a military clash on Damansky Island on the Ussuri River on the Russia-China border in Siberia, which ultimately resulted in China controlling the territory. The Soviet army, however, repelled Mao's attempt to make further inroads into Russia. A weakened Mao tried to initiate relations with Japan and the U.S., for whom it was a net strategic gain to separate the PRC from the Soviets.

After Mao died in 1976, his successor Deng Xiaoping sought to balance the old communist guard with reformers. He opened China to foreign investment and technology and implemented economic reforms. After normalizing relations with China, Japan provided development aid that today would be worth the equivalent of several trillion yen.

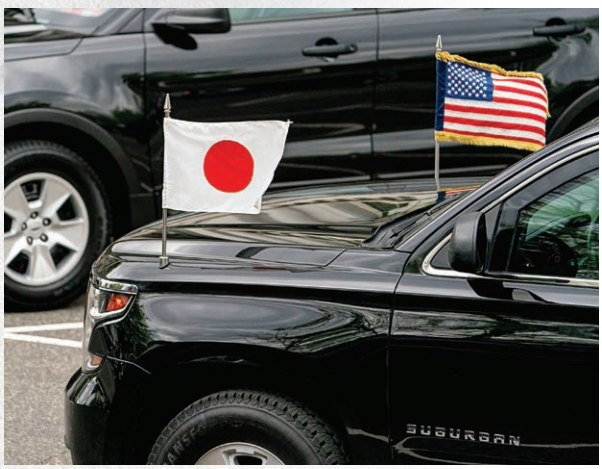
The end of the Cold War in 1989 brought the collapse of communist regimes throughout Eastern Europe, the Caucasus and Central Asia. Freedom's victory was celebrated around the globe, and a liberal atmosphere spread quickly. Those developments terrified the CCP's leadership. In response, Deng turned his back on democracy, pushing aside reformer Hu Yaobang, who had become his right-hand man. The events helped spark the 1989 Tiananmen Square protest by students who were calling for freedom and the subsequent massacre of civilians by the PLA in Beijing. Deng continued to accept foreign money and technology, however, and Japan continued to provide support after the massacre, believing that Deng was the only hope for reform and that the West should not drive China back to the extreme isolationism of the Mao era. In the end, China continued to lean toward the West.

The PRC took advantage of the West's open system and has emerged as a successful economy in the 21st century. Many believed that China would

become like the West one day. The expectation was bitterly betrayed. The CCP leadership feared losing power through the infiltration of Western liberalism. The CCP's fears only intensified as the communist ideology started fading as a result of Deng's reforms and the nation's economic development. The leadership needed a new legitimacy.

A Corrupt, Coerced Legitimacy

To create its supposed legitimacy, the CCP fabricated the legend of the glory of the party that is building today's China. The party uses selective history to emphasize the narrative. It cites such events as the Opium Wars, the Arrow Incident, the Sino-French War over Indochina, the Sino-Japanese War over Korea, the Boxer Rebellion and subsequent uprisings in Beijing, the loss of large parts of Siberia to the Russians, the Manchurian Incident by Japan, the Second Sino-Japanese War and the civil war with Chinese nationalist Chiang Kai-shek. The CCP seeks to evoke the emotions of the Chinese people by spinning its purported historical narrative as a tale of humiliation by foreign powers. This also stokes a sense of revanchism among the people.



The car carrying Yoshihide Suga, then Japan's prime minister, arrives at the White House in Washington, D.C., in April 2021 for Suga's meetings with U.S. President Joe Biden and U.S. Vice President Kamala Harris.

The legend is also used to fan the flames of nationalism. The CCP builds the glory of 5,000 years of Han civilization into its narrative. The tale can't survive academic scrutiny, but it is a political thought-control device necessary for the CCP's leadership. It also neglects the fact that the CCP inherited the Qing dynasty rather than the Han dynasty. Many northern ethnic groups, such as Mongols, Tibetans and Uyghurs, were key insiders in the Qing dynasty. Today, China's ethnic minority population exceeds 100 million, and they do not share Han nationalism. To counter this reality, the CCP has instituted their forcible and cruel assimilation.

The combination of a historical sense of revanchism and mounting nationalism propels the CCP's expansionism, in particular, its maritime expansionism. The CCP believes it must carve out a vast maritime area to defend the heart of China. It continues to militarize islets and shoals in the South China Sea, largely using its coast guard to seize and control territory. Since 2012, China has also been attempting to bully Japan, the main U.S. ally in the region, over the Japanese-controlled Senkaku Islands in the East China Sea.

CCP General Secretary Xi Jinping is adding new aggression to China's expansionism. Xi belongs to the extreme Maoist generation of Red Guards and does not share Western values. In fact, under Xi, the Chinese people are prohibited from discussing the universal values, such as freedom, democracy and human rights, that are championed in Western societies. By extending his term beyond 2022, Xi seeks to become a despot like Mao. And his trophy to outshine Mao could be the invasion of Taiwan.

Allying the West, Like-Minded Nations

No nation other than the U.S. is capable of facing China alone. China will likely become the world's biggest economy by about 2030. China, however, will not be bigger than the West if those nations are united and, especially, if they are joined by Australia, India, New Zealand and Southeast Asian nations in a club of freedom and democracy. The size of the PRC's population has already plateaued and is declining, which means that a united West allied with like-minded nations can still engage the PRC from a position of strength. How to realign the West is the first key strategic issue to address.

Then-Japanese Prime Minister Shinzo Abe first unveiled a Free and Open Indo-Pacific strategy in 2016. It proposed that Indo-Pacific nations, many of which are industrial democracies or at least free market supporters, should be realigned so that the growing region becomes a major piece of the liberal international order. The key alliances in implementing this strategy will be among Australia, Japan, South Korea and the U.S.

India, however, is the most important element for securing a successful Indo-Pacific strategy. It soon will surpass China as the world's most-populous nation, with an average age 10 years younger than that of China. India's economy, meanwhile, will surpass Japan's in 15 to 20 years. India has not forgotten the PRC's invasion of Tibet in 1950 and remains upset with the PRC's close relationship with Pakistan. Now that China stands against the West, India, although it is faithful to nonalignment diplomacy, is gradually shifting its weight toward the West and nations such as Japan and the U.S., with which it shares values.

Indian Prime Minister Narendra Modi, center, speaks during the virtual Association of Southeast Asian Nations' East Asia Summit in October 2021.

The future Western strategic framework with India will be based not only on strategic interests but also on the universal values.

As the threat posed by the PRC to the liberal international order becomes clearer, new and expanded groupings of like-minded nations are taking shape. For example, the Quadrilateral Security Dialogue, or Quad, should grow beyond its current members of Australia, India, Japan and the U.S. Those efforts should start with Europe, which has shared values and wields significant military and economic power. The new trilateral security pact among Australia, the United Kingdom and the U.S., known as AUKUS, will be a precious contribution to regional defense.

The 10-member Association of Southeast Asian Nations (ASEAN) represents a sizable and emerging regional force that should get more attention from the West. With a population about half that of China, ASEAN member states seek free trade partnerships, although their strategic interests vary, as do their threat perceptions. They do not want to be pulled into conflicts involving greater powers. At the same time, they are becoming wary of China's ambition to make them tributary states. Like Japan, Indonesia and the Philippines have never been tributary states of China. Vietnam, which threw off Chinese control in the 10th century, has a strong wariness of its big neighbor. Singapore and Thailand have a historical affinity with China, but they are allies or partners of the West. ASEAN has developed a splendid multilateral diplomacy with Western nations over the years, and many of its members are now proud democracies. For these reasons, the West must engage with ASEAN nations.

Preventing a Taiwan Contingency

The Indo-Pacific's biggest challenge in the 21st century is a potential Chinese invasion of Taiwan. Xi could seek to surpass Mao's legacy by realizing Mao's unattained dream of annexing Taiwan. The self-governed island of 23 million people is proud of its economic achievements and democracy. Its semiconductor industry, for example, is an indispensable part of the global supply chain. Taiwan is too valuable to lose to communist dictators who don't care about the freedom of Taiwan's people or the island's distinctive identity.

The West's status as a global leader is at stake: If Taiwan is lost, the world may view the West as having surrendered the entire Indo-Pacific to the Chinese dictatorship.

Taiwan is not an easy island to invade. It is the continuation of the Japanese volcanic archipelago next to Okinawa Islands. Mountains as high as 4,000 meters rise on the east side of Taiwan. It is a rocky island with limited places for amphibious attack. The CCP would not launch a full-scale military attack immediately. First, it would engage in gray zone activities. Beijing would also declare that any foreign intervention would violate the CCP's core interests and interfere in the domestic affairs of the PRC. The CCP would also denounce the use of force against it and declare that the safety of nationals of enemy states in China could not be guaranteed because of the rage of Chinese people.

An invasion of Taiwan is not likely in the next few years. But by 2027, when Xi's third term expires, Chinese military capability is projected to be such that the CCP could more successfully deter intervention by U.S. or other forces coming to the island's aid. At that time, an invasion will be a matter of when, not if, many experts agree.

Japan would be involved in such a crisis immediately for several reasons. First, China claims the Senkaku Islands as part of Taiwan. Second, Japan's Yonaguni Island and parts of its Sakishima Islands chain is 110 kilometers from Taiwan and would likely be within the war zone. Additionally, the CCP could seek to neutralize Japan Self-Defense Forces bases in the area. Third, the CCP may also seek to neutralize U.S. bases in Japan that would be used for operations to help Taiwan.

Japan's leadership has repeatedly said that peace and stability are essential to Japan's security. In the 2021 joint declaration between then-Prime Minister Yoshihide Suga and U.S. President Joe Biden, the same passage appeared. This is exactly what Japan had been saying with the U.S. before the Japanese-China and U.S.-China normalization. The U.S.-Japan Alliance treaty contains not only Article 5 that stipulates the obligation of the common defense of Japan but also Article 6 that stipulates that U.S. forces can use bases in Japan for the peace and stability of the so-called Far East.

The Far East in this context means the Korean Peninsula, the Philippines and Taiwan, which were left in a power vacuum when Japan was defeated in the Pacific War. The U.S. wanted to protect them using bases in Japan, and Japan thought the surrounding area of Japan should not be left unprotected in the face of massive red forces of China, North Korea and Russia. This is the regional security arrangement that was incorporated in the Japan-U.S. security arrangement from the beginning.

Soon after Japanese Prime Minister Fumio Kishida took office in early October 2021 after Suga stepped down September 3, he also met with President Biden to confirm Japan's commitment to strengthen the two nations' security alliance and cooperate on regional security.

Future Courses of Action

Much studying and heavy lifting remain to effectively deter China from invading Taiwan. There are many concerns to address. The following are the most fundamental ones.

First, the U.S.-Japan Alliance for the first time faces a substantial Chinese threat over Taiwan. China is far stronger than before, reaching U.S. economic size and building massive military forces. Japan's defense budget should be expanded drastically over 2% of GDP.

Japanese Prime Minister Fumio Kishida, left, and U.S. President Joe Biden greet with a fist bump at the NATO headquarters in Belgium in March 2022.

Second, the command line of the U.S.-Japan Alliance is not unified, as it is in South Korea or NATO. A scenario-based operational plan on a Taiwan contingency is required, and new roles and missions of both forces should be defined.

Third, strategic dialogue is necessary among Australia, Japan, Taiwan and the U.S. The U.K., as a member of AUKUS, would be a good partner. France would also be a good partner, given France is a Pacific nation. South Korea should be involved if the political will can be mustered.

Fourth, Japan's integrated operation capabilities should be strengthened. The integrated command of the Self-Defense Forces was established only in 2006, and the post of chief of staff of the Ground Self-Defense Force was created as recently as 2018. They should be made more robust as institutions.

Fifth, Japan has recently created a Marine Corps-like brigade within the Ground Self-Defense Force. It should be soon included in the integrated plan. □

Unusual Suspects

NONTRADITIONAL THREATS CHALLENGE INDO-PACIFIC SECURITY

FORUM STAFF

A pandemic entering its third year has shifted the outlook of Indo-Pacific defense practitioners. Security threats don't always take the shape of hostile troops, bombs or missiles. They are sometimes invisible, often naturally occurring and can be the result of bad actors taking advantage of a chaotic landscape.

Whether threats come from hackers capitalizing on an internet-dependent population or violent extremist organizations recruiting pandemic-weary malcontents, nontraditional threats are national and regional and must be countered with sophistication and resolve, experts agree.

The authors of a March 2021 report by CNA, a nonprofit research organization, said security ramifications caused by the pandemic are far-reaching and "almost no part of life has gone untouched by the virus."

"Historical perspective gained over time will assess the efficacy of the global response to this lethal virus," they said. "What already is clear, however, is that the COVID-19 pandemic has highlighted the complexities of safeguarding our national security while responding to a global health crisis."

CYBER THREATS ABOUND

Like the rest of the world, Indo-Pacific citizens moved their living, learning and working online during the pandemic, complicating an already risky cyber landscape. An increase in personal and business activity online exacerbated many cybersecurity challenges in the region, according to an April 2021 risk intelligence report by the online news magazine The Diplomat.

"Phishing emails continued to be a popular vector for cybercriminals to steal information from businesses, government agencies and civil society organizations large and small," The Diplomat reported in August 2021. "Businesses are increasingly digitizing their processes — again, a pre-pandemic trend — ranging from document-sharing to accessing user data, as more individuals get connected to the global internet by the year. Surveillance and privacy risks to individuals from both governments and companies were rising well before the COVID-19 pandemic, too."

Pandemic-era cybercrimes show that hacker activity is soaring.

- A North Korean hacker crew called Lazarus Group was accused of carrying out the biggest cryptocurrency heist of 2020 when it stole U.S. $275 million in virtual money from the KuCoin exchange, Forbes magazine reported in February 2021.
- The United States and its allies in July 2021 accused the People's Republic of China (PRC) of conducting a massive hack of Microsoft's email system and other ransomware attacks. The White House and governments in Europe and the Indo-Pacific issued a statement that accused China's Ministry of State Security of using "criminal contract hackers" to conduct destabilizing activities worldwide.
- The spread of COVID-19 brought a cybercrime wave to Singapore with a data breach at an employment agency and a massive ransomware attack on a specialty medical clinic, Techwire Asia reported in October 2021. Private information of Fullerton Health customers was stolen and hawked online after one of the health care company's vendors reported a data breach. Perpetrators put the data up for sale on hacking forums, The Straits Times newspaper reported. The hackers claimed they stole data from 400,000 people, including their insurance policy details.
- Officials escalated warnings about Moscow-backed cyberattacks against businesses and critical infrastructure worldwide following Russia's invasion of Ukraine in February 2022. "The magnitude of Russia's cyber capacity is fairly consequential," U.S. President Joe Biden said in March 2022.

In response to these threats, Indo-Pacific industry leaders are shoring up their cyber defenses. MIT Technology Review Insights surveyed 600 technology decision-makers in the Indo-Pacific and reported in December 2020 that more than three-quarters of their organizations had made digital investments to protect new ways of doing business. Six out of 10 respondents said they had business-continuity plans in place in the event of a cyber intrusion.

FERTILE GROUND FOR EXTREMISTS

COVID-19 is a textbook nontraditional threat — "an amorphous, evolving, and invisible adversary that proliferates without intention, bargaining or goals," according to the CNA research group. In its report, "Viral Extremism: COVID-19, Nontraditional Threats and U.S. Counterterrorism," CNA researchers found that traditional threats, such as terrorism, can thrive in the chaos a pandemic creates.

"COVID increases global instability. This is especially true, given the prolonged COVID experience brought on by waves of variants," Pamela G. Faber, one of the report's authors, told FORUM. "Violent extremist organizations and terrorist groups take advantage of, and actually try to amplify, environments of instability and chaos. This pandemic is exactly the type of environment in which these groups would thrive."

Faber, an expert in security and development in conflict and post-conflict regions, said COVID-19 creates threats to national, regional and global security by amplifying the risk of vulnerable populations being radicalized. "These risk factors include increasingly toxic and extremist online content, increased feelings of economic uncertainty, growing anger because of perceived government failures,

greater frustration because of perceived oppressive government responses, increased isolation from friends and feelings of loneliness, and higher levels of stress," she said.

In the Sahel region of Africa, for example, extremists exploited the pandemic by stepping up attacks on national and international peacekeepers, according to a June 2020 report in Modern Diplomacy magazine. "We are seeing attempts by terrorists and other groups in the region to capitalize on the pandemic to undermine state authority and destabilize governments," United Nations peacekeeping chief Jean-Pierre Lacroix told the U.N. Security Council in May 2020.

In the Indo-Pacific, Faber noted that the Islamic State group initially claimed the coronavirus was a punishment for China over its mistreatment of Uyghur Muslims. As the virus spread, however, the terrorist group began to describe COVID-19 as punishment from God on the West. Some extremist groups have also "used the pandemic to justify attacks against ethnic communities inaccurately labeled as responsible for the spread of the disease, particularly Asian communities," she said.

With some states and their defense forces overburdened by the pandemic or natural disasters, the Indo-Pacific is seeing plots forged amid strife. "Those involved in illicit activities are taking advantage of an environment where nations across the region are focused on immediate health threats over security," wrote J. "Lumpy" Lumbaca, professor of Indo-Pacific terrorism and irregular warfare at the Daniel K. Inouye Asia-Pacific Center for Security Studies, in an April 2020 report titled "Coronavirus, Terrorism, and Illicit Activity in the Indo-Pacific." Those trends continued throughout 2021.

Australia, Japan and the United States announced in December 2021 they would fund the development of 5G telecommunication networks in the South Pacific to hedge against the People's Republic of China gaining access to nations' critical infrastructure through Chinese tech companies such as Huawei. AFP/GETTY IMAGES

- Three Philippine civilians were killed in December 2021 when suspected communist rebels attacked government troops assisting the evacuation of Carmen, Surigao del Sur, ahead of Typhoon Rai, msn.com reported. Gov. Alexander Pimentel appealed to New People's Army rebels not to attack during preparations for the storm, which killed more than 400 people and displaced more than 135,000.
- In North Korea, border crossings to China were closed due to the pandemic, leaving desperate traders in North Hamgyong to turn to methamphetamine trafficking to survive, Lumbaca wrote. Although meth trafficking in North Korea is common, he said, local production increased when rumors spread that the drug could prevent or even cure the disease.
- State actors can also take advantage of the pandemic to silence dissent. In China, billionaire developer Ren Zhiqiang, known as "The Cannon" for his outspokenness, likened Chinese Communist Party General Secretary Xi Jinping to a power-hungry "clown" in a 2020 online post. He said the party's limits on free speech exacerbated the pandemic. Ren disappeared in March 2020, and the government in September 2020 announced he had been sentenced to 18 years in prison on corruption charges, The Associated Press reported. Ren had 37 million followers on Weibo, a Chinese social networking site. Many observers viewed the prosecution as retaliation. "Ren Zhiqiang is not a radical dissident, but a decades-long loyal Communist Party member who advocated for political reform," Yaqiu Wang, a China researcher at Human Rights Watch, told The New York Times newspaper. "The Communist Party has no tolerance of any kind of criticism toward the party, even if it is made with the intention to improve the party's governance."

FIGHTING NEW THREATS AS PARTNERS

From combating microchip shortages to distributing coronavirus vaccines, Indo-Pacific partners are addressing nontraditional threats. The leaders of Australia, India, Japan and the U.S. — members of the Quadrilateral Security Dialogue, or Quad — in September 2021 agreed to build secure semiconductor supply chains to counter a shortage that surfaced during the pandemic.

"Quad partners will launch a joint initiative to map capacity, identify vulnerabilities and bolster supply-chain security for semiconductors and their vital components," the White House said in a statement. "This initiative will help ensure Quad partners support a diverse and competitive market that produces the secure critical technologies essential for digital economies globally."

Microchips are the brains behind modern-day

A family seeks refuge in a makeshift shelter in Surigao, the Philippines, after Typhoon Rai in December 2021. Armed insurgents attacked Philippine troops evacuating residents ahead of the deadly storm. AFP/GETTY IMAGES

conveniences — everything from calculators and computers to satellites that enable GPS.

Quad countries also play a critical role in distributing COVID-19 vaccines. By September 2021, they had delivered nearly 79 million vaccine doses to the Indo-Pacific region and 1.2 billion globally, according to the White House.

The Serum Institute of India, the world's largest vaccine maker, resumed exports of coronavirus vaccines in November 2021 just as the omicron variant found in South Africa was beginning to cause worldwide concern. India had suspended vaccine exports in March 2021 following a surge in domestic cases. "This will go a long way in restoring vaccine supply equality in the world," Serum Institute chief executive Adar Poonawalla said on Twitter.

Through a U.S. $3.3 billion loan program, Japan continued to help regional countries procure vaccines, and Australia delivered U.S. $212 million in grants to buy vaccines for Southeast Asia and the Pacific region, according to the White House.

Protecting the free flow of information also is a priority for Indo-Pacific partners confronting nontraditional threats. Australia, Japan and the U.S. announced in December 2021 they would jointly fund the development of 5G communications networks in the South Pacific to hedge against the PRC gaining control of the region's critical infrastructure and potentially exporting its authoritarian values, Japanese news agency Kyodo News reported.

The decision was announced shortly after the three countries said they would help build an undersea cable network to improve the internet connectivity of the Pacific island nations of Kiribati, Micronesia and Nauru.

KEEPING COUNTERTERRORISM IN FOCUS

Even as partners coalesce to shore up supply chain vulnerabilities and defenses against rapidly spreading diseases, CNA researcher Faber contends defense planners need to stay focused on thwarting extremists who thrive in the midst of disaster. "Efforts to counter extremist groups must take into account the events and trends that bolster them," she said. "We have seen during COVID that the impact of nontraditional threats, such as pandemics, are very useful for these groups. Pandemics are just one type of nontraditional threat. Others include natural disasters, extreme weather, supply chain failures and natural resource scarcity. Crucially, understanding the impact of nontraditional threats on extremism has not historically been included in counterterrorism or counterextremism efforts."

She added that amplifying the role of prevention — countering violent extremism and radicalization — should be central to counterterrorism strategy, especially in the pandemic. U.S. counterterrorism efforts, for example, "should also recognize that some partner nations, especially those who are largely unable to meet the needs of populations in crisis, will be especially vulnerable to the impact of COVID on extremism." □

SECURITY THREAT

Prioritizing Climate Change in National Defense Strategies

FORUM STAFF

The vast Indo-Pacific sits at the forefront of critical climate challenges that contribute to conflict, instability and forced migration. Changes in the seas and oceans, in particular, pose an increasing security threat.

"Climate change-exacerbated impacts such as increasing food and water insecurity, forced migration and displacement, disaster response and recovery that does not meet expectations, and broader economic impacts can seriously complicate these existing security vulnerabilities — eroding coping capacities, increasing grievances and worsening underlying tensions and fragilities," according to "Climate and Security in the Indo-Asia Pacific," a report published in July 2020 by the International Military Council on Climate and Security (IMCCS). "Climate change impacts will interact with an evolving regional security landscape and likely give rise to new and potentially catastrophic risks, which could emerge in ways that are foreseeable but difficult to predict."

Indo-Pacific residents are five times more likely to be affected by a natural disaster than individuals living elsewhere, according to IMCCS, a group of senior military leaders, security experts and security institutions dedicated to anticipating, analyzing and addressing the security risks of a changing climate. The IMCCS was launched at The Hague, Netherlands, in 2019 in response to a growing demand from military professionals to share information and best practices to address the security and military dimensions of climate change.

"The world is at an inflection point for global climate action … we have witnessed a shift in awareness and growing acceptance of the security

Residents in Cambodia navigate a street flooded due to rising sea levels.

dimension of climate," according to the IMCCS's "The World Climate and Security Report 2021." The report stated: "It is now time to turn that awareness into action, driven by a sense of urgency amongst nations and other essential actors to address climate security risks."

Palauan President Surangel Whipps Jr. welcomes attendees to the Our Ocean Conference in Palau in April 2022. U.S. DEPARTMENT OF STATE

Military experts suggest strengthening the community of defense and security actors who examine how climate change affects the security environment. These individuals should be tasked with advancing ways to integrate climate-related threats into defense policy and planning and cultivating ways to share best practices and leverage expertise on resilience and humanitarian aid and disaster relief, according to climate experts.

"As a relatively new and dynamic non-traditional security issue, collaboration between security communities to understand and address climate security threats can improve preparedness for a changing security environment," according to the IMCCS Indo-Asia Pacific report.

NO TIME TO WAIT

Regional groups have long kept climate change at the head of their discussions on national security and multinational cooperation. The Pacific Islands Forum, for example, has worked to maintain a strong and coordinated voice for the 18 Pacific island nations that comprise the forum in negotiating resources to combat climate change.

"Pacific Islands Forum leaders recognize climate change as the single greatest threat to our region," Henry Puna, the forum's secretary general, said at the 26th United Nations Climate Change Conference, or COP26, in Glasgow, Scotland, in November 2021. "While there has been progress in the negotiations, more needs to be achieved."

COP26 concluded with more than 100 world leaders pledging to end deforestation by 2030 to slow climate change. Among the Indo-Pacific signatories are Australia, Bhutan, Brunei, China, Fiji, Indonesia, Japan, Nepal, New Zealand, Papua New Guinea, the Philippines, South Korea, Sri Lanka, the United States and Vietnam. In a statement, the signatories called their pledge essential to meeting the goals of the Paris Agreement, an international treaty adopted by 196 parties in 2015 to limit global warming to well below 2 degrees Celsius.

The Our Ocean Conference in April 2022 produced a six-point action plan to combat ill effects on the world's water bodies and garnered more than 400 commitments worth U.S. $16.35 billion from countries worldwide to protect ocean health and security.

"Island nations are on the frontlines of the dual ocean and climate challenges," said Palauan President Surangel Whipps Jr., who co-hosted the conference with John Kerry, U.S. President Joe Biden's special envoy for climate. "By hosting the meeting, Palau was not only able to show the world just how vulnerable we are to these crises, but also the many solutions available to tackle the problems today if we just choose to use them."

Whipps called the threat facing Pacific nations real, saying coordinated action is needed to turn the tide.

"Oceans and coastal communities bear the brunt of climate change," Whipps said, challenging Palauans and people worldwide to be part of the solution. "Our connection to the ocean is very personal. It's our home. It's our lifeline. It's what makes us who we are."

Kerry emphasized the U.S.'s commitment to conquering climate change. The oceans are "the great climate temperature regulator," he said. "These commitments tackled some of the greatest threats to the ocean of our time," Kerry said. "They addressed plastic pollution. They addressed illegal, unreported and unregulated fishing. They addressed the climate crisis. Not just words, but actions."

Since 2014, the Our Ocean Conference has generated more than 1,800 commitments worth about U.S. $108 billion.

Scientific forecasts indicate that climate change through 2040 will have a more severe impact on countries including North Korea and several developing nations in South and Southeast Asia, according to a U.S. National Intelligence Council National Intelligence Estimate. Vulnerabilities to climate change could also create internal conflicts and increase the risk of instability in developing nations, including small island nations across the Pacific Ocean, according to the October 2021 report.

"More broadly, developing countries are likely to need to adapt to a mix of challenges that climate change will exacerbate. Ineffective water governance in developing countries will increase their vulnerability to climate effects, undermining livelihoods and health. Some will face new or more intense diseases and lower yields from existing staples of their agriculture," according to the report, titled "Climate Change and International Responses Increasing

A man walks past a house abandoned after it was flooded due to rising sea levels in Central Java, Indonesia.
THE ASSOCIATED PRESS

Challenges to U.S. National Security Through 2040." "In addition, insurgents and terrorists may benefit. We assess that most of the countries where al-Qaida or ISIS [Islamic State of Iraq and Syria] have a presence are highly vulnerable to climate change."

Evidence suggests that natural disasters can be a precursor for an outbreak in terrorism, according to "Agenda For Change 2022: Shaping a Different Future For Our Nation," a study published in February 2022 by the Australian Strategic Policy Institute (ASPI). The report noted spikes in terrorism in Sri Lanka and Thailand following the 2004 Indian Ocean tsunami.

"The warming climate will cause unprecedented economic and social disruption in our region, particularly in countries such as Indonesia and the Philippines, with significant socioeconomic vulnerabilities," the ASPI report stated.

Indonesia and the Philippines account for 90% of the people living below the poverty line in Southeast Asia, according to ASPI. Employment across the region is in informal sectors, with no official social safety nets to support large populations displaced by disasters, the report said.

"Inequality is increasing, and ethnic and religious tensions have previously led to major outbreaks of violence, separatist movements and terrorism," according to the ASPI report. "It's likely that climate disruptions will reverse the recent regional decline in terrorist incidents and attacks."

ECONOMIC IMPACT

The Secretariat of the Pacific Regional Environment Programme (SPREP), a joint initiative based in Samoa and composed of intergovernmental organizations for sustainable development, has focused on environmental impacts to the livelihoods and heritage of the Pacific since the 1970s. In its "Strategic Plan 2017-2026," SPREP stated climate change is already affecting coastal and forest ecosystems, oceans, freshwater supplies and biodiversity, particularly in communities in small, low-lying countries where sea level rise and changing weather patterns have created social and economic disruption.

"Pacific island countries are striving to balance the needs and economic aspirations of their growing populations on the one hand, with the maintenance of healthy environments and natural systems on the other," according to SPREP's plan. "Our ability to address these threats together, to craft cooperative and sustainable

Only a small pile of rocks remains above the water line at low tide on this uninhabited island on Majuro atoll in the Marshall Islands, as rising seas erode coastlines and contaminate freshwater wells. THE ASSOCIATED PRESS

solutions, build on the opportunities provided by ecosystem services and secure political commitment, will determine the future for Pacific islands people."

Through 2026, SPREP's focus areas include climate change resilience, ecosystem and biodiversity protection, waste management and pollution control, and environmental governance. Although the COVID-19 pandemic presents challenges for collaboration and implementation of plans, SPREP's leadership remains committed to the mission.

"The fear and uncertainty of what is ahead is only natural, especially since we have all witnessed how things have dramatically changed during the past two years as a result of the pandemic," Kosi Latu, SPREP's director general, said in a January 2022 message on the organization's website. "Still, we are here. In uncertain times like today, we need to be resilient; we cannot give up; we are duty bound to adapt, adjust and persevere."

Latu and others say it's past time that talk transitioned to action — and many agencies have already made the leap.

"Governments, institutions and individuals are taking action to mitigate the risks of climate change. New policies are being put in place, health care systems reformed and innovative solutions to tackle the negative effects of climate change created," according to Asia Society Switzerland, a global network advancing dialogue and strengthening partnerships in Switzerland and Asia. "But a great deal remains to be done — and there is no time to wait."

MISSING IN ACTION

While most militaries around the world adjust to limit their carbon footprint, the People's Liberation Army (PLA) has remained largely silent about its climate strategy.

Chinese Communist Party (CCP) General Secretary Xi Jinping has pledged to reduce China's carbon output starting in 2030 and achieve carbon neutrality by 2060, "but little has been heard from the PLA's senior leaders, academics and strategists," Defense One reported in January 2022.

"While climate change is a part of the Chinese military and militia's concept of non-traditional security threats, addressing its effects does not yet appear to be part of its security strategy," according to Defense One.

The PLA quietly acknowledged climate change as a security concern in a 2010 white paper on national defense, following decades of reluctance to do so, according to the blog Lawfare.

"China's shift from skeptic to true believer on climate change and security is not, for the most part, because leadership has suddenly become convinced that climate

change is real," a 2019 Lawfare post noted. "China is already affected by worsened floods, more extreme droughts, diminished fishery productivity and other ecological changes. The government has long understood that a warming climate will threaten the country's agricultural production, make economically important cities vulnerable to catastrophic flooding and eventually dry out many of the country's rivers."

China's major urban economic centers are mostly along its eastern coast and the river valleys that flow into it, according to Defense One. Because of population patterns, studies suggest that rising seas will displace at least 30 million people in China by 2050, Defense One reported. PLA facilities and forces are also at risk of displacement, including installations built on artificial reefs in the South China Sea.

"The PLA established a committee of climate experts 13 years ago, but it does not appear to be active. Climate change went unmentioned in the PLA's 2019 Defense White Paper. Nor does the PLA appear to be taking the ever-increasing threats of environmental catastrophe seriously as part of [its] training or strategic outlook," Defense One reported. "There has been no public discussion of exercises or attempts to wargame the effects of climate change on China's security environment. Nor does construction appear to be slowing down on island installations in the South China Sea, despite the fact that many will find themselves underwater when the ice caps melt."

Despite the lack of transparency by the PLA and CCP on climate action, analysts believe Xi must worry that climate change will affect his One Belt, One Road infrastructure scheme. "Chinese companies, citizens and the state itself are increasingly exposed to climate-related security issues such as extreme flooding and drought, migration and protests over Chinese-financed infrastructure construction," according to Lawfare. "It is no exaggeration to say that, in the coming decades, China's response to climate change as it relates to agriculture, water and flooding will have profound impacts on billions of people."

Additionally, environmentalists blame PRC-built dams along the Mekong River for contributing to historic flooding and droughts that have harmed the fish population and negatively impacted the livelihood of those who depend on the Mekong for food and income. "Regardless of how much rain falls during the wet season, upstream dam restrictions are devastating for the Mekong's ecological success and the natural resources that come from the river upon which tens of millions rely," Brian Eyler, director of the Southeast Asia program at the Stimson Center, told the German news site DW.

Beijing denies its dams are the cause of the collapse in fishing stocks and other issues downstream, according to NBC News. In late 2020, the PRC created an online platform to share information about the river's flow year-round. Critics say sharing data doesn't change the reality of life in the region and the negative consequences that continue because of the dams.

"We see that there are agreements and promises from China to share information, but this is insufficient," Pianporn Deetes, campaign director for International Rivers, an environmental conservation organization based in California, told DW. "Someone telling us they're turning on or off the tap is not helpful. The Mekong and its people need natural and ecological flow in order to sustain the natural services."

AN EXISTENTIAL THREAT

President Biden's administration in October 2021 released a detailed plan for U.S. government agencies to implement climate change adaptation and resilience plans. The goal: Integrate climate-readiness across the missions and programs at all levels of government, including the military.

"Climate change is an existential threat to our nation's security, and the Department of Defense (DOD) must act swiftly and boldly to take on this challenge and prepare for damage that cannot be avoided," U.S. Secretary of Defense Lloyd Austin said in a statement about the DOD's adaptation plan. "We do not intend merely to adapt to the devastation of climate change. We will work with nations around the world to meet the threat."

Austin called climate change a destabilizing force that demands new missions and an altered operational environment. Extreme weather events affect troop readiness and drain resources, he said. Going forward, the DOD will include security implications of climate change in all risk analyses, strategy development and planning. It will also incorporate climate risks into modeling, simulations and wargaming.

"Developing sound intelligence estimates and decision-making tools about an inherently uncertain future where some specific climate changes are likely, yet not specifically known, requires both discipline and flexibility. Threat analysis, modeling and simulation, wargaming, and experimentation enhance the Department's understanding of its current and future operating environments," according to the DOD's 2021 Climate Adaptation Plan. "Harnessing artificial intelligence to develop predictive models and decision support tools for operational and business decision-making processes can inform planning and operations in the U.S. and abroad."

The DOD plan calls for collaborating with allies and other nations on new technologies, building partner nation capacity to respond to climate change-related hazards and working with communities adjacent to U.S. military installations to build shared resilience and enhance shared ecosystems.

"Planning for today and into the future is our business," Austin said, "and we would not be doing our job if we weren't thinking about how climate change will affect what we do." □

STRATEGIC PARTNERS IN

SPACE

U.S. SPACE COMMAND STRENGTHENS INDO-PACIFIC ALLIANCES

U.S. SPACE COMMAND

The United States and its allies and partners have established a network during the past 70 years that provides a unique, competitive advantage over common adversaries. Every day, defense partners share intelligence, train together and collaborate to create combined capabilities that far exceed what each country can accomplish alone.

Worldwide interest in space enables the U.S. to broaden and deepen its international partnerships while opening new avenues for collaboration. Access to outer space contributes substantially to life on Earth. Space-enabled technologies provide critical, yet often unrecognized, support for daily activities. Technological advances and lower costs drive society to be more reliant on space-based capabilities, and a loss of access would have far-reaching effects. Position, navigation and timing services, for example, provide critical support to modern infrastructure. Without precise timing, financial institutions could not create time stamps for transactions, hindering the use of ATMs and credit cards. Utility companies would be unable to manage and distribute critical resources. The space environment is evolving rapidly, presenting the U.S. and the international community with key challenges.

Shared concerns over security threats create the foundation for strong alliances and partnerships. Key challenges include orbital debris and the development and deployment of anti-satellite (ASAT) capabilities. The People's Republic of China (PRC) is a focal point of concern. The PRC officially advocates for the peaceful use of space, but it continues to surreptitiously test and improve its counterspace systems while enacting reforms to better integrate cyberspace and electronic warfare in space into joint military operations.

A Falcon 9 rocket carrying satellites launches from Cape Canaveral Air Force Station in Florida in January 2020. It was the first official launch of the United States Space Force. U.S. SPACE FORCE

The PRC has rapidly aligned civil and military activities to expand its presence in space, and its space program has been responsible for uncontrolled descents, dangerous debris-producing ASAT tests and the fielding of a hypersonic glide vehicle capable of long-term orbit and long-range strikes. U.S. Secretary of Defense Lloyd Austin, in his keynote speech at the Reagan National Defense Forum in December 2021, said the PRC is "increasingly focused on integrating its information, cyber and space operations."

> Worldwide interest in space enables the U.S. to broaden and deepen its international partnerships while opening new avenues for collaboration.

As the world witnessed after the PRC's ASAT weapon test in 2007, counterspace weapons testing can have disastrous and lasting results. The test created more than 3,000 pieces of orbital debris, and much of that debris cloud is expected to stay in orbit for decades, threatening the International Space Station and other spacecraft. NASA's Crew-3 mission was forced to maneuver the space station in November 2021 to avoid debris spawned by the PRC's ASAT weapon test.

The debris, which came from a remnant of a Chinese weather satellite destroyed by a missile, was on a path to enter a rectangular zone 4 kilometers deep and 48 kilometers wide around the space station, NASA reported.

Before 2007, most space debris was attributed to space launch vehicles. Today, over one-third of

debris is caused by events such as the PRC's 2007 destruction of an orbiting satellite. While Beijing continues to pursue its goal of dominating space, the future of a peaceful and prosperous space domain relies on a global coalition of free nations dedicated to the tenets of responsible space behaviors.

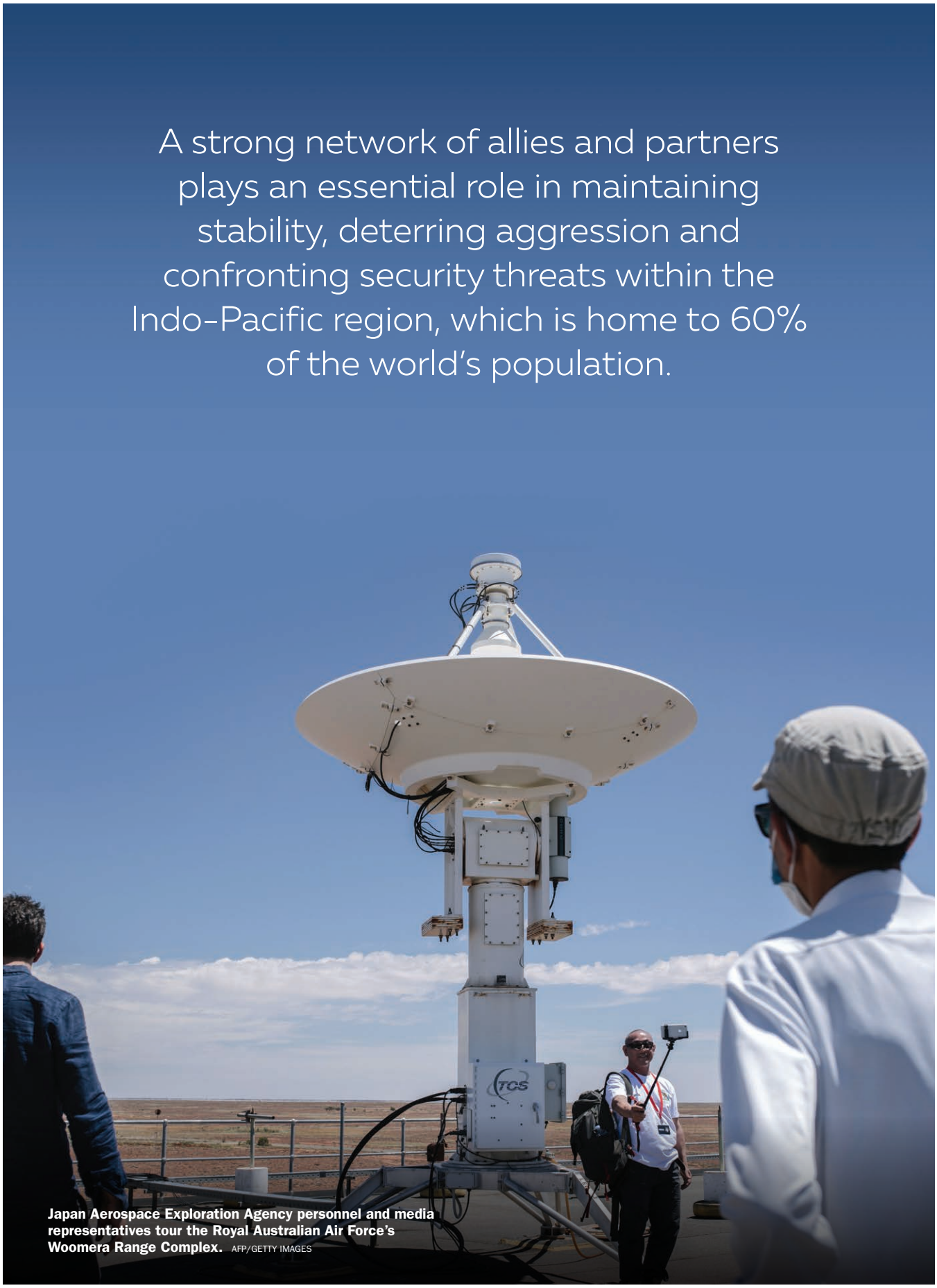
A strong network of allies and partners plays an essential role in maintaining stability, deterring aggression and confronting security threats within the Indo-Pacific region, which is home to 60% of the world's population. The U.S. continues to build and maintain key relationships with like-minded nations throughout the region. U.S. Space Command (USSPACECOM) nurtures these relationships primarily through Space Domain Awareness (SDA) agreements, exercises and infrastructure sharing.

USSPACECOM maintains over 25 SDA agreements with partners across the globe, including Australia, Japan, New Zealand, South Korea and Thailand. There are tens of thousands of objects in orbit that pose a potential threat to satellites and launches. SDA refers to tracking those objects and predicting their position at a given time. Indo-Pacific countries, including Australia, Japan and South Korea, participate in exercises such as Global Sentinel that highlight the seamless interoperability among participating nations.

USSPACECOM continues to seek opportunities to partner with other Indo-Pacific nations to promote responsible behaviors in space. Allies and partners are critically important, and USSPACECOM continues to strengthen its network in an era of strategic competition. In October 2021, Maj. Gen. DeAnna Burt,

Personnel at the Royal Australian Air Force's Woomera Range Complex prepare for the arrival of asteroid samples collected by a Japan Aerospace Exploration Agency probe. AFP/GETTY IMAGES

A strong network of allies and partners plays an essential role in maintaining stability, deterring aggression and confronting security threats within the Indo-Pacific region, which is home to 60% of the world's population.



Japan Aerospace Exploration Agency personnel and media representatives tour the Royal Australian Air Force's Woomera Range Complex. AFP/GETTY IMAGES

This can't be accomplished without the steadfast support and commitment of allies and partners in the Indo-Pacific and worldwide.

South Korea launches a single-stage rocket from the Naro Space Center. South Korea and the United States have a Space Domain Awareness agreement for tracking objects in orbit. AFP/GETTY IMAGES

Yuichi Tsuda, second from right, discusses Japan's project to collect asteroid samples. Tsuda was manager of the Hayabusa-2 project for the Japan Aerospace Exploration Agency. AFP/GETTY IMAGES

commander of the Combined Force Space Component Command, visited South Korea to further strengthen the U.S.-South Korea alliance. South Korea has achieved milestones in its advancement of space, including standing up its first space operations squadron and launching its first dedicated military satellite. "Without international cooperation and partnerships forged by leaders within the enterprise, space would be impossible," Burt said, according to a U.S. 7th Air Force news release. "Partnerships are imperative for success."

USSPACECOM also hosted Australian Army Lt. Gen. Gregory Bilton, Australia's chief of joint operations, to reaffirm the importance of space cooperation between the two nations.

Winston Churchill, prime minister of the United Kingdom during World War II, famously stated: "There is only one thing worse than fighting with allies, and that is fighting without them." This quote rings just as true today as in 1945. The shared system of alliances and security partnerships has afforded enormous strategic advantages to the U.S. and other Indo-Pacific nations. Emerging strategic competition has added to the scope and scale of the challenges facing the U.S. and its allies and partners. To deter aggression, there must be a resilient space security posture, and partners must have the ability to detect and attribute hostile acts in space.

This can't be accomplished without the steadfast support and commitment of allies and partners in the Indo-Pacific and worldwide. Deterrence in space requires credibility and legitimacy of cross-domain responses to aggression — an approach greatly enhanced by alliances. With these unshakable alliances, Indo-Pacific partners will launch a peaceful and prosperous future that expands well beyond the limits of geography. □

PRESERVING THE RULES-BASED INTERNATIONAL ORDER

U.S. NAVY CAPT. (RET.) RAUL PEDROZO

THE U.S. FREEDOM OF NAVIGATION PROGRAM PROMOTES REGIONAL SECURITY AND STABILITY

All nations benefit from a Free and Open Indo-Pacific region governed by the rules-based maritime order that sets out an acceptable legal framework for all uses of the world's oceans. Despite the vital role this order plays in promoting peace and security and advancing economic prosperity in the region, the international order is under serious attack. States such as the People's Republic of China (PRC) and Russia seek to impose a new order — one based on "might makes right" — advancing maritime claims that are inconsistent with international law. The United States' freedom of navigation (FON) program is one available tool to counter these attacks on the established international order, and it underscores the U.S. commitment to preserving a stable legal system for the world's oceans for all nations.

The FON program was initiated in 1979 after then-U.S. President Jimmy Carter's administration determined that written diplomatic protests were ineffective in reversing excessive maritime claims and that a more tangible demonstration of U.S. resolve was needed to influence nations to either avoid new unlawful assertions or renounce existing ones. The adoption of the United Nations Convention on the Law of the Sea (UNCLOS) in 1982 was touted as a comprehensive, widely accepted international framework governing uses of the oceans that carefully balanced coastal and maritime states' interests.

Although the U.S. was instrumental in developing most of the convention, then-U.S. President Ronald Reagan declined to sign it because of untenable flaws in Part XI on deep seabed mining. Nonetheless, President Reagan indicated in his 1983 Ocean Policy Statement that the U.S. would recognize the rights of other states in waters off their coasts, as reflected in UNCLOS, so long as such coastal states recognize the rights and freedoms of the U.S. and other nations under international law.

The U.S. Navy guided-missile destroyer USS John S. McCain transits Peter the Great Bay in the Sea of Japan while conducting routine operations. PETTY OFFICER 2ND CLASS MARKUS CASTANEDA/U.S. NAVY

President Reagan, however, also issued a warning to states that, despite being a party to UNCLOS, continued to assert maritime claims that were inconsistent with the convention. Reiterating the importance of the FON program, the Ocean Policy Statement indicated that the U.S. would not acquiesce in illegal acts by states designed to restrict the international community's navigational rights and freedoms, and that the U.S. would "exercise and assert its rights, freedoms, and uses of the sea on a worldwide basis" consistent with the balance of interests reflected in UNCLOS.

PRESERVING ACCESS FOR ALL

The FON program operates along three tracks: diplomatic communications by the U.S. State Department, bilateral consultations with other governments, and operational assertions by U.S. naval ships and military aircraft. Since the program's inception, the U.S. Navy and U.S. Air Force have conducted hundreds of operational assertions globally to demonstrate U.S. nonacquiescence in excessive maritime claims designed to restrict navigational rights and freedoms and other internationally lawful uses of the seas.

Contrary to allegations that the FON program is provocative and could result in unintended consequences, freedom of navigation operations (FONOPS), in essence, are a nonprovocative exercise of rights, freedoms and lawful uses of the sea and airspace guaranteed to all nations under international law, including UNCLOS. FONOPS are deliberately planned, legally reviewed, properly approved by higher authority, and safely and professionally

A U.S. Marine Corps F-35B fighter jet prepares to launch from the United Kingdom's newest aircraft carrier, HMS Queen Elizabeth, during a replenishment with vessels from the U.K. Royal Navy and the Royal Netherlands Navy in the South China Sea in July 2021. The vessels were part of a U.K.-led international carrier strike group mission to uphold freedom of navigation in the Indo-Pacific region under the United Nations Convention on the Law of the Sea. PETTY OFFICER JAY ALLEN/U.K. ROYAL NAVY

conducted in a nonescalatory manner. The program is applied globally and is not based on political events or the identity of the nation advancing an illegal claim. In 2020, for example, the U.S. challenged the excessive claims of 19 nations, including adversaries (e.g., Iran and the PRC), allies and friends alike. Routine application of the program to all nations maintains its legitimacy and nonprovocative intent and demonstrates U.S. resolve to preserve access to the world's oceans for ships and aircraft of all nations.

The PRC and Russia also routinely contend that they have "expelled" U.S. warships conducting FONOPS from their claimed territorial waters. Such disingenuous assertions are cheap propaganda designed to inflame nationalist sentiment at home and misrepresent lawful U.S. maritime operations. In the 40-plus years of the FON program, no U.S. warship has been expelled from a coastal state's waters. If challenged by coastal state authorities, U.S. warships reply that they are simply conducting a lawful operation in accordance with international law and then continue on their designated course until the mission is complete. In 1988, two Soviet warships intentionally rammed the USS Caron and USS Yorktown while they were conducting a FONOP off the Crimean Peninsula. Despite the collision and repeated threats from numerous Soviet vessels, the U.S. warships continued their track until they exited the Soviet-claimed territorial sea after completing a 75-minute transit.

The 1988 Black Sea incident is a vivid example of how the FON program can be used to preserve navigational rights and freedoms. It reinvigorated bilateral discussions between the two superpowers regarding the legal aspects of innocent passage that had been ongoing since 1986. The discussions led to the signing of the 1989 Uniform Interpretation of Rules of International Law Governing Innocent Passage, known as the Jackson Hole Agreement, in which the Soviets agreed with the U.S. position that "all ships, including warships, regardless of cargo, armament or means of propulsion, enjoy the right of innocent passage through the territorial sea in accordance with international law, for which neither prior notification nor authorization is required."

COUNTERING THE PRC'S EXCESSIVE CLAIMS

The U.S. Secretary of the Navy's new Strategic Guidance, issued in October 2021, reiterates that the U.S. will expand its "global posture to ensure the presence of naval forces with the right mix of platforms, capability, and capacity to maintain freedom of the seas, support international law and norms, stand by our allies, and continue to fly, sail, and operate wherever international law allows." A robust FON program is one pillar of that

A U.S. Marine Corps F-35B from Marine Fighter Attack Squadron 211 prepares to land aboard the United Kingdom Royal Navy aircraft carrier HMS Queen Elizabeth during multilateral freedom of navigation operations in the South China Sea. PETTY OFFICER JAY ALLEN/U.K. ROYAL NAVY

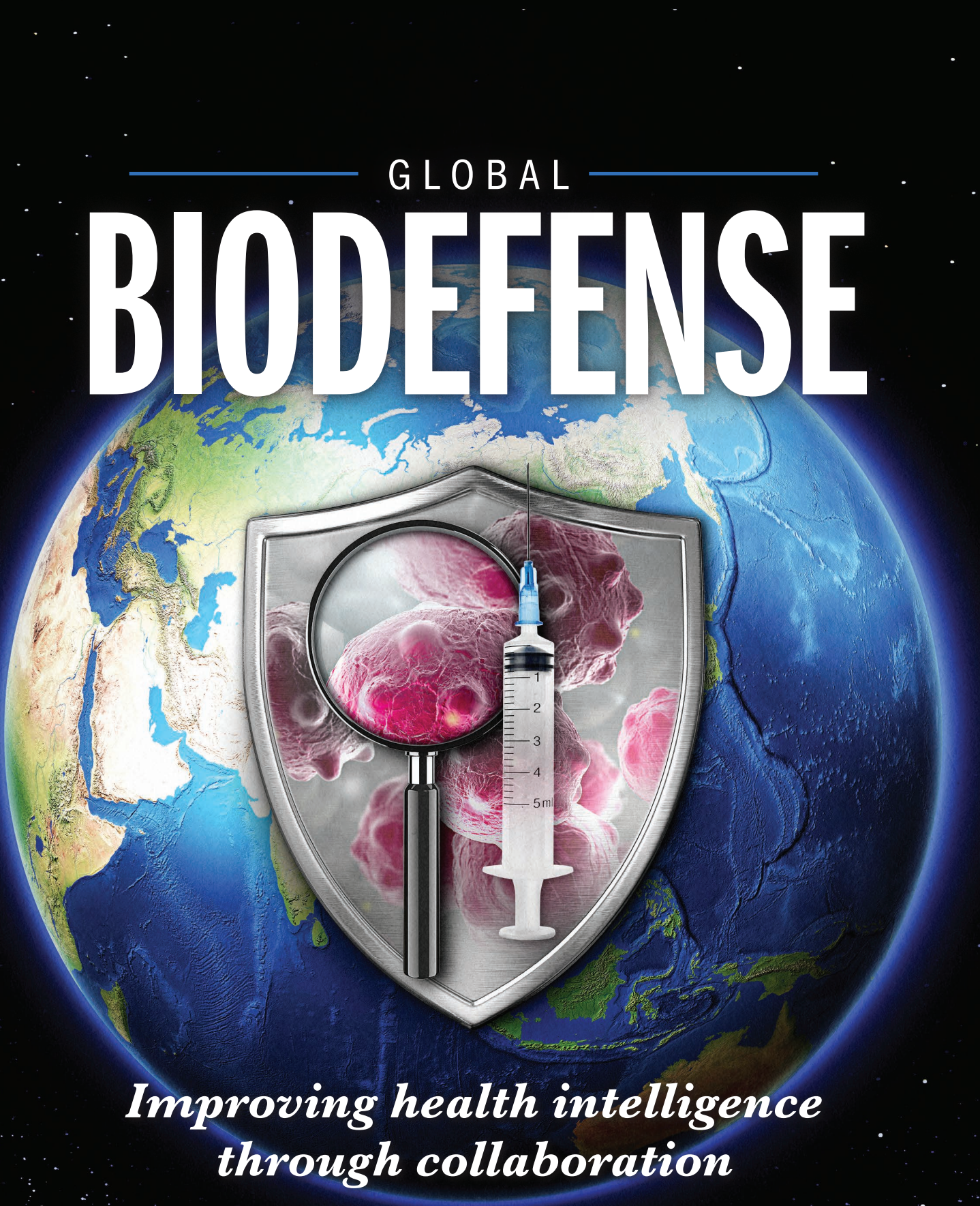
expanded global posture, which aims to counter the proliferation of excessive maritime claims that restrict access to the world's oceans. Left unchallenged, these excessive maritime claims can infringe the rights, freedoms and lawful uses of the sea enjoyed by the U.S. and other nations. In short, the FON program underscores the U.S.'s willingness to fly, sail and operate wherever international law allows and exemplifies its unwavering commitment to a stable, rules-based legal system for the world's oceans.

This is particularly true in the South China Sea where the PRC routinely flouts international law and engages in dangerous and provocative actions to advance its unlawful maritime claims and intimidate smaller states from lawfully exploiting their maritime resources. In 2016, an international tribunal ruled unanimously that there was no legal basis for the PRC to claim maritime rights in the South China Sea based on its infamous nine-dash line. The tribunal also determined that the PRC's large-scale land reclamation and construction of artificial islands at the seven features it occupies in the Spratly Islands caused severe harm to the marine environment and violated the PRC's obligation to preserve and protect fragile ecosystems. The ruling is legally binding, but Beijing has refused to comply with it. Since 2016, the U.S. has conducted more than 30 FONOPS challenging the PRC's excessive maritime claims in the Spratly and Paracel islands.

The international community has an enduring obligation and responsibility to preserve the freedom of the seas, which is critical to global security and prosperity. The U.S., therefore, encourages nations to conduct their own freedom of navigation operations and to publicly oppose excessive maritime claims that impede navigational rights and freedoms. In as much as some countries continue to claim and assert restrictions on navigational rights and freedoms that exceed what is provided for under international law, the U.S. will continue to demonstrate its resolve to uphold the rules-based order that has proven essential to securing global security, stability and prosperity for all nations. □

GLOBAL

BIODEFENSE



Improving health intelligence through collaboration

FORUM ILLUSTRATION

U.S. NAVY REAR ADM. (RET.) MICHAEL BAKER, JACOB BAKER, DR. DEON CANYON AND DR. SEBASTIAN KEVANY

Intelligence gathering that includes disease surveillance is an important early warning tool that strengthens decision-making capability and national security. United States military forces, medical assets and intelligence agencies — and those of its allies — are crucial for early detection and response in the fight against emergent disease outbreaks. These factors underscore the need to establish a biodefense fusion center.

U.S. intelligence agencies, laboratories, civilian institutions, assets of U.S. allies and partner nations, social media and data mining can be interwoven with technology and leveraged for mutual defense. The basic pillars of an early warning system are already in place and must be better funded and coordinated going forward.

Alliances, partnerships and interconnectivity need to be improved and coordinated among governments, independent social media data miners and other assets that can support this mission. These efforts need increased funding and intensive collaboration to weave their information into an international biodefense shield with U.S. security partners.

Zoonotic transmission from animals to humans, lab accidents or biowarfare can trigger an outbreak, and disease can quickly spread globally as experienced with the COVID-19 pandemic. COVID-19 has also shown crucial U.S. national security vulnerabilities and shortfalls in the response capability of the U.S. and its allies and partners. Adversaries have likely taken note.

Military and civilian intelligence agencies seek foreign source information developed from rapidly ramped-up efforts during World War II. The U.S. Central Intelligence Agency (CIA) was established in 1947 and began producing medical intelligence reports focused on communist bloc capabilities and trends, while the U.S. Army Medical Intelligence and Information Agency handled the related military medical intelligence. The latter evolved into the U.S. Armed Forces Medical Intelligence Center and later was designated the National Center for Medical Intelligence (NCMI) to reflect the organization's wider constituency, which now includes the White House, the U.S. departments of State and Homeland Security, other agencies, domestic customers and international partners.

As the U.S. Department of Defense's (DOD's) lead agency for producing medical intelligence, the NCMI is responsible for coordinating and preparing integrated, all-source intelligence on foreign health threats and other medical issues to protect U.S. interests worldwide for the DOD and other government and international organizations.

Chemist Yoshito Oshiro gathers samples for testing at the 18th Aerospace Medicine Squadron at Kadena Air Base, Japan.
SENIOR AIRMAN JESSICA H. SMITH/U.S. AIR FORCE

Given that diseases are transboundary in nature, it is essential that the U.S. can detect them before they reach U.S. soil. The problem is that many closed nations, such as China, Iran, North Korea and Russia, are not transparent about medical issues that affect their citizens and could affect other nations, such as a disease outbreak. Information about transmissibility, genome data and virulence statistics is crucial for combating disease outbreaks but characteristically difficult to obtain.

Synthetic bioweapons could enable a new capability — weapons that render threat detection difficult, have no conventional equivalent and are harder to counter.

The value of these tools was evident in November 2019 when the U.S. intelligence community and the NCMI began to warn of a global epidemic, saying that the COVID-19 outbreak in China could develop into a cataclysmic event. Policymakers, decision-makers and the U.S. National Security Council were repeatedly briefed on the issue. By early January 2020, the COVID-19 outbreak had been mentioned in the U.S. president's daily brief of national security matters. In this pandemic, government intelligence agencies and military medical intelligence gatherers were well ahead of the curve in raising the alarm.

FUTURE THREATS

Synthetic bioweapons (SBWs) are weaponized biological vectors modified through synthetic biology for novel effects, mechanisms or processes. For example, CRISPR-Cas9, an acronym for clustered regularly interspaced short palindromic repeats (CRISPR) and CRISPR-Associated Protein 9, is a genetic editing technique that has cured diseases in humans, but it can also be used to create SBWs. In addition, SBWs could enable a new capability — weapons that render threat detection difficult, have no conventional equivalent and are harder to counter.

Doctrinally, China has recognized the critical role that unconventional weapons might play, and some Chinese have already rejected moral limits on SBWs. China must be prepared to synchronize all government capabilities at all levels of competition, with all tools considered legitimate, according to the 1999 book "Unrestricted Warfare" by Qiao Liang and Wang Xiangsui, colonels in the People's Liberation Army Air Force.

FORWARD-LOOKING BIODEFENSE ASSETS

The U.S. military, in conjunction with its intelligence resources, a revitalized U.S. Centers for Disease Control and Prevention and global institutions, can provide the building blocks for an early warning and rapid response system woven into a national biodefense fusion center. The DOD has forward-deployed bases, forces, labs, hospitals, intelligence assets and surveillance resources, all backed by an agency that has demonstrated success in early warning, testing and response measures. In 1998, five organizations within the DOD collaborated to create the Defense Threat Reduction Agency (DTRA) to better synchronize plans and actions for nuclear deterrence, weapons of mass destruction and biothreats. The DTRA quickly provided subject matter expertise, portable lab testing facilities, vaccines and treatments for an Ebola outbreak in West Africa.

The DOD's overseas laboratories research infectious diseases of public health and military importance. The DOD's global emerging infections surveillance and response system includes the following agencies, several of which are World Health Organization (WHO) Collaborating Centers:

- Armed Forces Research Institute of Medical Sciences, Thailand
- U.S. Army Medical Research Unit, Kenya
- U.S. Naval Medical Research Unit, Italy
- U.S. Naval Medical Research Unit, Cambodia
- Naval Medical Research Center Detachment, Peru

A biotechnologist processes blood samples at a Singapore laboratory. REUTERS

These overseas military facilities form the basis for an effective international infectious disease surveillance effort, especially when collaborating with civilian health agencies such as the WHO, partner nations and nongovernmental disease outbreak search platforms.

INTERNATIONAL OPEN-SOURCE TOOLS

The Epidemic Intelligence from Open Sources (EIOS) program is a collaboration among public health stakeholders globally for early detection, verification, assessment and communication of public health threats by using publicly available information. EIOS is based on the early alerting and reporting project of the Global Health Security Initiative and the hazard detection and risk assessment system (HDRAS), as well as work with global initiatives such as the Program for Monitoring

Medical teams from Singapore and Thailand simulate cardiopulmonary resuscitation during field training at Cobra Gold 2020. PETTY OFFICER 1ST CLASS OMAR POWELL/U.S. NAVY

Emerging Diseases (ProMED), the Global Public Health Intelligence Network (GPHIN), HealthMap and the Europe Media Monitor.

The GPHIN is a web-based program established in the late 1990s that uses a network of multinational and multilingual professionals to rapidly detect, identify, assess and mitigate threats to human health. It is a crucial part of the WHO-developed HDRAS, which uses web-based epidemic intelligence tools and collects information from HealthMap and ProMED, among others. HealthMap uses informal online sources for disease outbreak monitoring and real-time surveillance of emerging public health threats, including the mobile app Outbreaks Near Me. The International Society for Infectious Diseases launched ProMED in 1994 as an internet service to identify unusual health events related to emerging and reemerging infectious diseases and toxins affecting humans, animals and plants.

Open-source intelligence tools used for health surveillance automatically collect and collate data, thereby evaluating much larger quantities of information with algorithms and producing relevant reports. GPHIN, ProMED and HealthMap have provided alerts on some of the most serious disease outbreaks in the past two decades. For example, despite its earlier experiences with severe acute respiratory syndrome (SARS), China did not report a November 2003 human H5N1 influenza case until 2006. Yet, by evaluating content from Chinese media and low-level online chatter, ProMED provided the first English-language alert of SARS and prompted confirmation by the Chinese government. Similarly, indicators of a recent Ebola outbreak were detected by HealthMap before any announcements by officials or the WHO. And EIOS picked up the first report of a cluster-type pneumonia outbreak in Wuhan, China, on December 31, 2019 — an outbreak that would become the COVID-19 pandemic.

FUTURE STEPS

The U.S. National Security Strategy (NSS) provides a framework for protecting the nation and ensuring its freedom, security and prosperity in a rapidly changing, complex world. Consistently and innovatively translating the NSS blueprint into action remains a core function of government.

It is time for the U.S. to spearhead the development of a biodefense fusion center. This initiative is urgently required to meet growing transboundary infectious disease threats to international security.

Even in extremely challenging operational theaters, the use of medical diplomacy initiatives through military global health engagement has been a highly effective peacekeeping tool.

National biodefense must not be exclusively reactive. Research needs to be undertaken by organizations such as the DOD's Defense Advanced Research Projects Agency's (DARPA's) biotechnology office. DARPA will need the resources — more funding and personnel — to drive the development of advanced biosensors, diagnostics, countermeasures and other defenses to keep pace with changes in diseases. This has become even more urgent now that designer weapons can be created. Another asset is the DTRA, whose mission "enables DOD and the U.S. government to prepare for and combat weapons of mass destruction and improvised threats," including those of biological origin.

A comprehensive counterpandemic and counter-SBWs plan would look for and respond to clear and present biological dangers while advancing the operating country's knowledge about disease potential and emerging threats. The U.S. government must develop flexible, rapid and effective response plans that include well-maintained stockpiles of specialized sensors, protective equipment and medications.

BIODEFENSE FUSION CENTER PARTNERS

The U.S. could advance disease surveillance, reporting and early response with a biodefense fusion center by leveraging existing security relationships with regional allies and partners in a coordinated approach to improve domain awareness and communication. Intelligence asset reporting, health and lab information, and social media and big data searches from an array of sources must be collated, validated and rapidly disseminated to provide biodefense.

U.S. Navy Lt. Keerstin Whitefield, left, and U.S. Army Capt. Alison Crowe, center, participate in a medical knowledge exchange with nurses at Tuy Hoa Hospital, Vietnam, as part of Pacific Partnership. PETTY OFFICER 3RD CLASS CHANEL TURNER/U.S. NAVY

Partner nations could help build a disease early warning system, as demonstrated by Indo-Pacific countries that have a major stake in disease surveillance and early warning. These nations are already significantly aligned with the U.S. through organizations such as the Daniel K. Inouye Asia-Pacific Center for Security Studies.

Health surveillance and security can be quickly interconnected by leveraging the member states of the Quadrilateral Security Dialogue, or Quad — Australia, India, Japan and the U.S. — and the Five Eyes intelligence-sharing alliance of Australia, Canada, New Zealand, the United Kingdom and the U.S. This can form the basic pillars of a biodefense shield as information is directed to the biodefense fusion center. In much the same way, national and international maritime fusion centers are being proposed to reduce transnational threats at sea.

Potential partners in a more robust, regional biodefense fusion center and biodefense shield could include Japan, South Korea, Taiwan and Vietnam. Other nations such as India, Israel and NATO and European Union member states could be included to form a global and comprehensive disease surveillance enterprise. Current events have demonstrated that such alliances are both proactive and successful at mitigating pandemic problems.

The next iteration of U.S. strategy must focus on key collaborative initiatives that collate and fuse data from intelligence sources, health assets and social media web crawlers to tease out new or evolving threats to health and security. Drawing on the strength and strategic alignment of existing relationships will only be effective with rapid intelligence sharing across platforms. Therefore, the U.S. approach needs to be innovative and ensure that critical instruments of alliance power are leveraged quickly to facilitate appropriate responses to health threats with adequate scope and focus.

RESOURCE COMMITMENTS

Global health intelligence in the 21st century is an increasingly important part of national security, strengthens national defense and requires a greater share of the resources committed to conventional warfare. Through soft power and health security functions, it also protects national security directly and indirectly.

Even in extremely challenging operational theaters, the use of medical diplomacy initiatives through military global health engagement has been a highly effective peacekeeping tool. Medical and disease threat intelligence is, thus, vitally important to the safety and security of a nation and its people. Military forces, health departments, labs and civilian intelligence agencies need funding and staffing beyond the levels seen during the COVID-19 pandemic.

Infectious diseases are evolving and disrupting nations at a faster pace. This is exacerbated by demographic, political and climate change pressures that push populations into wilderness or other areas once considered uninhabitable. Thus, potential exposure to novel agents rises with population growth. The next pandemic may strike a human population exposed due to rapid, unsustainable urbanization, climate change, destructive food harvesting and production practices, globalization and reliance on other nations for essential items.

Philippine Air Force 1st Lt. Racy Dalida prepares an anesthetic for a patient during a cooperative health engagement as part of Exercise Balikatan. CPL. TIMOTHY HERNANDEZ/U.S. MARINE CORPS

The development of effective global systems for managing infectious disease surveillance and health intelligence is challenging, but excellent tools and agencies are available, and new tools are constantly emerging. The goal is to establish a global, collaborative surveillance and reporting mechanism, fund it generously and staff it with the best talent. This is not a project that needs to be started from the ground up, as many of the necessary assets and partnerships to build a collaboration already exist. The U.S. is well-positioned to grasp the baton, reframe military and security thinking and resource allocation in the health security context, and lead the next steps in global early warning and biodefense. □

This article was originally published in September 2021 by the Daniel K. Inouye Asia-Pacific Center for Security Studies (DKI-APCSS) publication Security Nexus. It has been edited to fit FORUM's format. The views expressed are the authors' alone and do not necessarily reflect the official position of DKI-APCSS.

ADVANCING SPECIAL OPERATIONS

INSIGHTS ON LEADING A NEW COMBATANT COMMAND AND THE IMPORTANCE OF PARTNERSHIP

FORUM STAFF

MAJ. GEN. FRANCISCO ARIEL A FELICIDARIO III, Commander of the Armed Forces of the Philippines Special Operations Command (AFP SOCOM), sat down with FORUM for an interview April 1, 2022, the fourth anniversary of AFP SOCOM, during the 37th iteration of Balikatan, a joint exercise of the Philippines and the United States. The celebration capped the AFP's announcement that SOCOM had become a combatant command. SOCOM gained operational control of the Marine Special Operations Group, the Naval Special Operations Command, the Philippine Air Force Special Operations Force and the Philippine Army Special Operations Force in 2018.

Felicidario became SOCOM commander in January 2022 after holding key positions in the Philippine Army and at the AFP General Headquarters, including chief of staff, Training and Doctrine Command, and executive officer of the Office of the Assistant Chief of Staff for Operations and the Office of the Deputy Chief of Staff for Operations.

He began his career in the Philippine Army after graduating from the Philippine Military Academy in 1989 and served as a Scout Ranger for more than a decade, later serving as a Scout Ranger Battalion commander from 2010-12. He also commanded two brigades in Mindanao in 2018 and was named acting assistant division commander in 2019 before being reassigned to the National Capital Region as the chief of the AFP Peace and Development Office. Among his many honors and awards, Felicidario earned two Distinguished Service Star Awards, a Bronze Cross Medal and a Meritorious Achievement Medal.

Philippine Naval Special Operations Command SEALs participate in a capability demonstration in Manila, the Philippines.


REUTERS

Why did you gravitate toward special operations throughout your career?

It's exciting to be with special operations. It was especially exciting during my lieutenant days when I was with the Rangers. Besides for the actual service … the Rangers, then as independent companies, are always deployed whenever there's a heightened conflict. Whenever there is a heightened conflict in Sulu, you get to be deployed there for eight months or so or more. And then when the conflict shifts to another area, you go to that place, whether it's in Vesavas or in other provinces, so it was exciting for a lieutenant during those days and after as a captain and a major.

And later on, we worked for counterterrorism (CT) operations and the development of special operations (SO) for the Philippine Army.

I had a front-row seat on how we would structure our capabilities for special operations, so I appreciate very much how important it was for AFP to be able to develop its own special operations forces (SOF) capabilities.

As the AFP builds out joint and combined capabilities, how will this affect your command?

It will be actually a big change in our way of planning, our progress, our future. I really battled for the command to be renamed as a combatant command, because when the AFP special forces were being stood up, somehow, we were put into the category of the AFP-wide service support unit. I said that would derail much of any progress in development because a service support unit is really different from being a combatant command unit. All your projections for probable capability development and so on would not be made available immediately to you. We are happy that we are now renamed and recognized as a combatant command, special operations command.

The development will surely be focusing on new trends for special operations. We are now talking even with our U.S. counterparts during the Balikatan exercise about exploring the other special operations fields apart from counterterrorism.

We're talking about the imminent threats to maritime security and how special operations forces will address it, and even using Ukraine as a model for how SOF were able to mobilize the whole country to fight. So those are things that now SOCOM can fully engross itself in to try to conceptually, at first, develop what special operations for AFP will be five, 10 years from now to be able to address future threats or imminent threats to the country both internally and externally.

With Balikatan 2022 focusing on joint training, will you talk to the value of bilateral training in achieving your aspirations to work with allies and partners?

For a long, long time, it's undoubtedly been a big help. When I was with the training department for the Philippine Army, I was the one in charge of Balikatan for the Philippine Army and for most of the bilateral individual training as well for the IMET [international military education and training] courses. I was the one processing officers and sending them to schooling in the U.S. for the IMET-themed courses at the same time doing unit as well as bilateral training. We were heavily involved as part of the G8 Philippine Army.

As far as the development goes — skill, competency wise — it's good to be able to do it, although on a training level with other countries that have more advanced experience in those particular fields and compare how your capability is progressing.

And they say it goes both ways because of the experience that we have while having been in the fight for so many decades already. It's the marriage of the experience of AFP troops being in constant fighting for our country against the insurgency and counterterrorism, and the technologies and the new capabilities and skills that our bilateral partners like the U.S. bring to us.

That marriage of competency, skill and the actual experience has emerged well into bringing forth the actual development and imparting the skills and the competencies of our Soldiers. And we just hope that somehow, our experience actually works well also with how our U.S. partners' counterparts are able to perceive bilateral training as a benefit to them also.

Discuss the importance of AFP SOCOM working with U.S. and other countries' special operators to enhance SOF capabilities in the region.

The value for us is the U.S. is very experienced in special operations. We have our experience as far as our own special operations for counterinsurgency and our own conflicts. But the U.S. has been to many places and has varied SOF experiences. The doctrines for the U.S. and other countries have been well-developed already. That would surely be without saying it's a benefit for the Filipino SOF forces if we would learn from it. That alone is a big contribution for having bilateral engagements: to have the U.S. speaking to us.

And of course, the knowledge of how the different innovations in technology in warfighting integrate with special operations. And once we see the equipment being brought by the U.S. and how they are able to utilize the equipment for special operations, even our organization program for SOF will have a certain focus. Experience using it together with U.S. counterparts will help us. We also train with the Australian SAS [Special Air Service Regiment] as far as special operations counterterrorism exercises.

Philippine and U.S. forces celebrate the fourth anniversary of the Armed Forces of the Philippines Special Operations Command on April 1, 2022, at Fort Magsaysay, the Philippines.
ARMED FORCES OF THE PHILIPPINES

Philippine Navy SEALs storm a beach during a simulated extraction of a kidnapping victim at the Philippine Marines training center in Ternate.
THE ASSOCIATED PRESS

Philippine Naval Special Operations Group members, who fought Islamic State-linked Muslim militants in Marawi in the southern Philippines, flash the victory sign after disembarking from the Philippine Navy amphibious ship BRP Tarlac in October 2017. THE ASSOCIATED PRESS

Tell us more about your Joint Operations Concept and how exercises, engagements and exchanges help you implement this?

For now, it's in the infancy stages of its operating concepts as far as the Armed Forces is concerned because we've actually stood up our area commands already as the joint operating commands. Operations are usually heavily ground forces with the Air Force just being in a support role and the Navy in a support role. It's not really coequal.

But it's changing now because the Air Force and the Navy are acquiring new platforms. That's why the bilateral training is a big help also. As we acquire the new platforms, we need the competency to be able to use the new platforms, which fortunately the U.S. military can give us.

This modernization program is being undertaken and now bringing fruits, so to speak, with the new platforms coming in. It would now capitalize the development fully of our joint operating concepts. And we could further maximize the writing of our own doctrine for joint operations with the new platforms in mind, especially now that we are using the new platforms already. Over time we'll see the full evolution of joint operating concepts of the AFP as we integrate new platforms.

Please talk to the importance of balancing internal CT requirements with the ability to respond to external threats.

While still in office, [then-President Rodrigo Duterte] declared a full campaign to hopefully end insurgency, so most of the focus is actually on CT and counterinsurgency for now. All our units are busy.

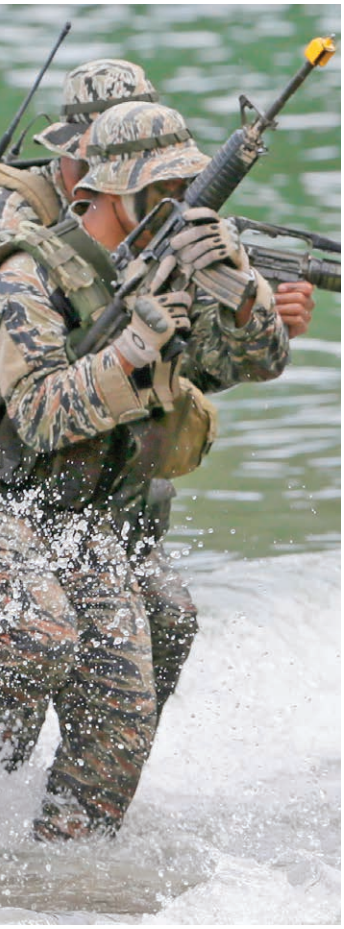
But there is a component of each of the major services that remains focused on external threats, such as maritime warfare. A good portion is already dedicated, and on the conceptual level there are think tanks within the major services and the GSU [General Staff University] already that are trying to see where we will be and how we will tackle external threats after counterinsurgency with the full force.

For balance, it's heavily on counterinsurgency and CT with dedicated people looking into the external affairs and threats and how we should address them at the conceptual level at least.

When we talk about capability buildup, it's a way that we are actually acquiring assets that we can use for external defense, but once they arrive, they could also be used for internal threats immediately. So that is a balance of what we are doing with how we are procuring for our organization at the moment.

What are the main challenges for AFP SOCOM?

For now, in its infancy, SOCOM has to be fully capacitated to handle all the SOF challenges that could come our way. But the good thing about it is that all the SOF units of the major services are already fully



capacitated in the areas of CT and counterinsurgency. They are fully competent now.

What needs to be capacitated, partly because it's only in its fourth year, is this command. But as far as the competence of the Soldiers, the officers are there already. We can meet the challenges. It is no problem.

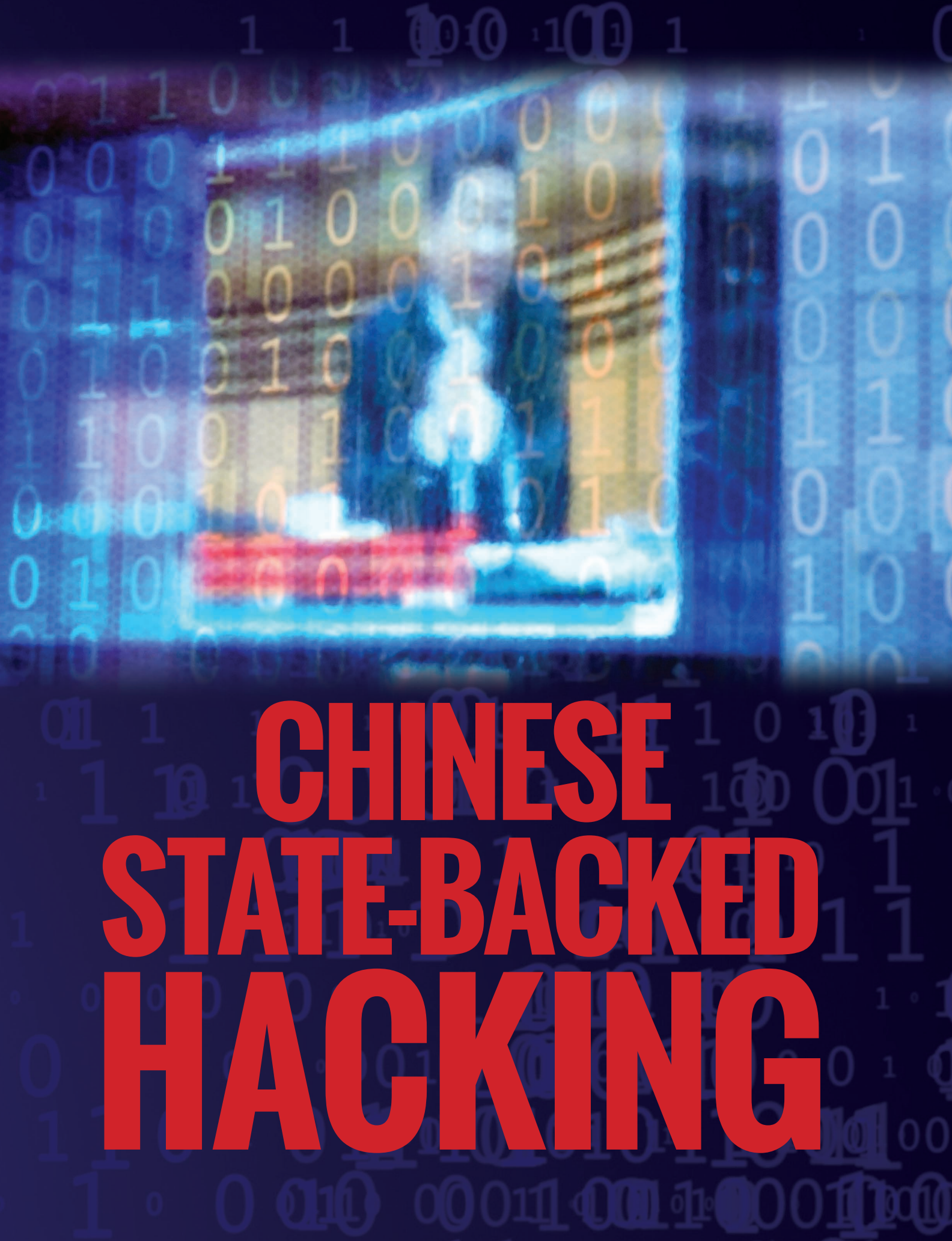
Even if we are too heavy right now in CT, counterinsurgency, we'll start at least at a conceptual level discussing and capacitating ourselves for trying to think on how we will be addressing external threats as far as SOF operations are concerned. The West Philippine Sea [also known as the South China Sea] will be one of the focuses of special operations of conceptual development. The Western frontier of our seas in Cebu and Tawi-Tawi. All our border areas. And then of course SOF requirements for unconventional warfare. Taking the Ukraine crisis as an example of how SOF are being utilized in capacitating the people to be able to fight, this was actually an area of competence of Philippine Soldiers … when it was guerilla warfare during World War II, for example. We should be able to go back to the competencies again if the need arises. Like it is a need now for Ukraine to fight for its freedoms, Filipinos have experienced that kind of fighting before and we must go back to those competencies.

Where I am focusing now is what is the challenge for five years, 10 years, 20 years … given the challenges for SOF given the insurgency will wind down. My staff is focusing on the SOF requirements to address any threats the country needs to counter in the future and working with the U.S. and other nations for planning and training our forces in areas that include cyberterrorism, use of UAVs [unmanned aerial vehicles] for special operations. I already talked to our artillery to start training with them to ensure they are able to integrate with us. I talked to our armor division already and told them that some portion of armor should be used to operating with SOF in the event we must integrate armor and SOF it will not be a problem. I have also talked to the Airborne Regiment. I already brought the idea that most of our non-SOF units need to be able to integrate with SOF and train together to improve our interoperability of forces.

Is there anything else you'd like to share with FORUM?

On a last note, I'd like to thank the U.S. government and the U.S. Armed Forces for their continued support to the Philippines as we move to more robust talks on how we will do the Mutual Defense Treaty if it comes to that and try to prepare as we are preparing now on the side of special operations. We have started talking for maritime SOF, external threat special operations and the like.

It's a big, big help to us that the U.S. continues to be a friend and a presence here in the Philippines with us. □



CHINESE STATE-BACKED HACKING

Time to level the playing field and breach the 'Great Firewall'

MICHAEL SHOEBRIDGE

More than 30 countries across Europe, North America and the Indo-Pacific in July 2021 joined in revealing and condemning the Chinese Ministry of State Security's work with Chinese cyber hackers and cybercriminals to hack companies, governments and other organizations globally, stealing valuable intellectual property and conducting ransomware attacks.

The grouping included Japan, the United States and, through NATO, 28 European nations, as well as Australia, Canada and New Zealand.

Far from being an issue involving only Beijing and Washington as part of strategic competition between two great powers, this behavior from the Chinese state shows that China poses a systemic challenge to all open societies. It's not a surprise that this large and growing group of governments is working more closely together to face it. It's the same grouping we saw coming together on China at the G-7-plus meetings in Cornwall, England, in June 2021.

Chinese state actions and the government's cooperation with China's criminal hacker "ecosystem" are damaging and flagrant. That's not news. So, what do we do?

We need to start by realizing that this is not just a case of Chinese authorities tolerating cybercriminals operating out of China. The Chinese government is working with and through its criminal cyber community to advance its interests and damage others — corporations and governments alike. That damage is to every one of the countries that spoke out in July 2021 and to companies operating in their economies.

There are four big messages out of this for governments and companies.

The first is to take in the implications of this deeply malign, damaging behavior of the Chinese state, which professes peaceful intent and an abhorrence of interfering in other jurisdictions, and to think through the specific risks and damage that can result. This is a board- and CEO-level issue for every Australian company, for example.

The second is for governments and companies to tighten their cybersecurity by implementing the detailed set of mitigating measures the U.S. and partner cybersecurity agencies set out in support of the July 2021 joint statement. Three big things to do are: getting software patches up to date to remove vulnerabilities; increasing internal system monitoring to spot malicious and suspicious activity inside networks; and using antivirus software along with a domain reputation service (to spot activity coming from malicious or suspicious sources before it compromises systems).

These steps will make it harder for China's Ministry of State Security and the cybercriminal outfits it works with to penetrate and compromise systems internationally.

The last two messages are arguably much more challenging and more important.

The global attacks were about China hacking into foreign digital technology — in this case, Microsoft Exchange systems used in much of the advanced world — with the attackers looking for valuable information as well as vulnerabilities in how companies' and governments' critical digital systems work. That's a bad problem to have.

But consider the enormous additional vulnerabilities that any government, critical infrastructure operator or government agency faces by using Chinese-sourced digital technology. The Ministry of State Security doesn't need a hacker network to get into these systems. As the Australian Strategic Policy Institute's series of reports on the expansion of China's tech giants shows, the ministry can go straight through the front door, accessing and using data produced by the normal business operations of Chinese digital systems and, when it needs to, compelling the secret cooperation of Chinese vendors and operators.

That gives companies and governments a sobering risk to factor in when making decisions about digital technology and software adoption, along with the usual

Opposite page: Chinese Communist Party General Secretary Xi Jinping is featured on a screen through digitally decorated glass during an internet conference in Wuzhen, China. REUTERS

Japan Aerospace Exploration Agency staff members run a safety check at the Institute of Space and Astronautical Science in Sagamihara near Tokyo. Hackers linked to the Chinese military launched cyberattacks in 2021 on hundreds of Japanese companies and research organizations, including the space agency. THE ASSOCIATED PRESS

business-case elements of cost, performance and ease of implementation.

National 5G and digitization initiatives, along with specific critical and digital infrastructure decisions — whether on transport, communications, public health or e-commerce — must now take account of not just the risk of hacking, but the risk of inherent compromise of digital supplier and operating organizations.

The last big message from this wholesale Chinese hacking enterprise is that it's time to stop accepting that open economies and societies are somehow uniquely vulnerable and that all we can do is make ourselves harder targets, soak up these Chinese (and Russian — remember Solar Winds) attacks and express concern.

More targeted indictments and asset freezes on Chinese officials — such as leaders and operatives in the Ministry of State Security — and charges against Chinese cybercriminals will help. Stronger corruption laws in more countries, including Australia, must be part of the answer. But that won't be a big enough deterrent by itself.

In light of the systemic challenge that China under Chinese Communist Party (CCP) General Secretary Xi Jinping poses, it's time to give Beijing some home games and homework to do.

China's digital ecosystem is messy, patchy and vulnerable. It requires legions of humans to keep spotting gaps and fixing seams, as well as to operate and police. Plus, we know how vulnerable the CCP regime feels to anything but well-chewed, censored information reaching the 1.3 billion Chinese citizens who are not party members.

Listening to Xi's CCP centenary speech in July 2021 reminded anyone who had forgotten that a central thought he and other CCP leaders have every day is the need to continue to struggle to stay in power. So, ensuring only the "correct line" is provided in China's information space is a continuing huge priority for Xi.

The same is true, strikingly, for President Vladimir Putin in Russia, whose recently released national security strategy sees the "home front" as the most dangerous and critical one for him to control to stay in power, given the threat of foreign ideas and information that challenge his narratives. While commentary has been about Russia's use of cyber and disinformation power against others, the vulnerabilities in Russia's cyber and information space worry Putin more than most other threats. Xi seems to suffer the same anxieties, as did his predecessors.

The governments that are routinely targeted by Beijing can work together and independently to stand up China-focused outfits with missions like Radio Free Europe, creating and using capable digital-era approaches to routinely breach the Chinese government's "Great Firewall." This can provide sources of external information and commentary, as well as footage of Chinese security thugs beating up Hongkongers and operating arbitrary interrogation centers, of the People's Liberation Army massacring Chinese students in Tiananmen Square in 1989 and of eyewitness testimony about the graphic mass abuses Chinese officials are committing against Uyghur Muslims every day.

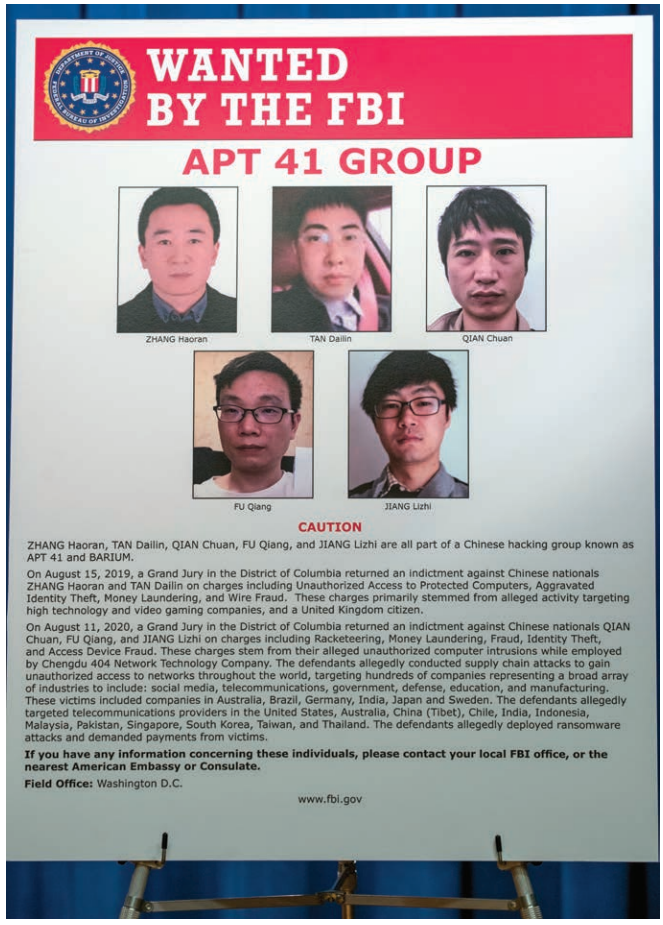
Some healthy doses of China's history, including the mass deaths Mao Zedong inflicted on China's people through his Great Leap Forward, will contest the propaganda-driven, aggressive nationalism Xi and his leadership colleagues stoke.

This will provide a partial antidote for the historically ridiculous notions that all China's troubles have been inflicted by evil foreigners, and that the party is the Chinese people's benevolent protector. The contrast with the stage-managed happy, dancing Uyghurs and the silence and denials of other CCP abuses will be confronting and jarring to Chinese citizens and amplify the power of this external information.

We know there's an appetite for this kind of information — and for discussion within mainland China and with people in places such as Taiwan and elsewhere — from the example of the short-lived Clubhouse app, where this kind of conversation happened before Chinese censors banned it in early 2021.

While we're thinking through how to demonstrate to the Chinese government its own vulnerabilities as part of stronger deterrence, it would be useful to ensure that Beijing understands it has myriad critical infrastructure and digital vulnerabilities.

Having Beijing know the practical reality of this and be anxious about vulnerabilities that it doesn't know about, but which capable governments might, could be the kind of tangible constraint Xi and his colleagues best understand. This is a future for cyber deterrence.



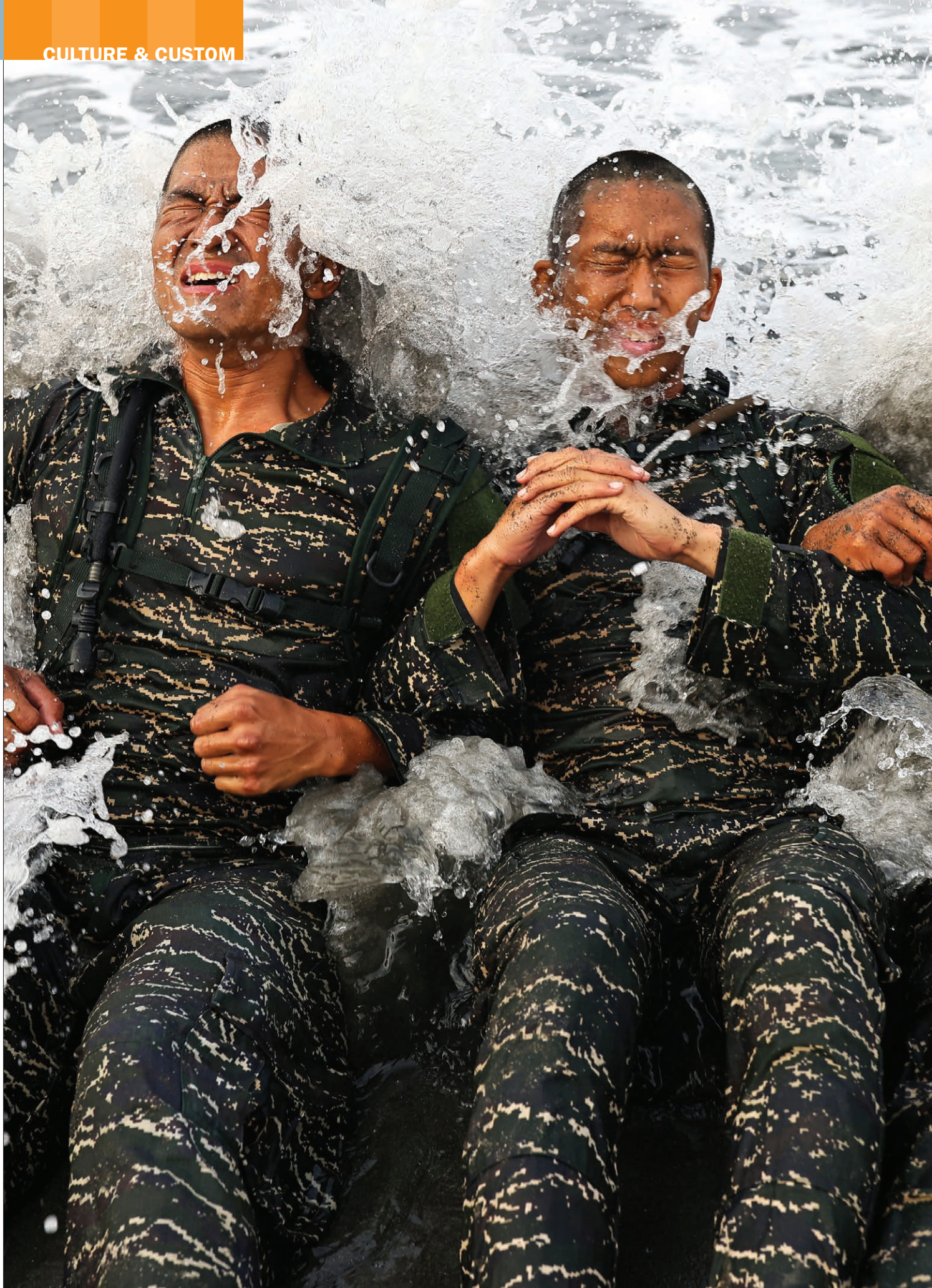
The U.S. Justice Department charged five Chinese citizens in September 2020 with hacks targeting more than 100 companies and institutions in the United States and abroad, including video game companies, universities and telecommunications providers.
THE ASSOCIATED PRESS

This coordinated response from the democracies hopefully ends the approach whereby governments, including in Canberra, would say nothing publicly about extensive Chinese state cyber intrusions while pretending that wider relations with Beijing could progress as normal.

There can be no return to a trusting "win–win" relationship with Beijing at the same time as we are being spied on and robbed blind by its hackers.

The nasty implications of this most recent exposure of Chinese state and criminal cooperation are much wider than just providing more work for cybersecurity professionals and concerned foreign affairs departments. It's a further step along the path of growing international cooperation to deal with the systemic challenge of China. And it's time to show that the digital playing field isn't all tilted in Beijing's favor. □

Michael Shoebridge is director of the Australian Strategic Policy Institute's (ASPI's) defense, strategy and national security program. This article was originally published July 20, 2021, in the ASPI's online forum, The Strategist. It has been edited to fit FORUM's format.



Taiwan frogmen train to

LEAP INTO ACTION

STORY AND PHOTO BY REUTERS

A chill wind whips across the Taiwan Strait as a small group of Taiwan Marines stands shivering on a remote dock in the early morning, their shorts and thin jackets drenched after a day spent mostly in the sea.

"Are you a sleeping beauty? Are you skipping out on class?" a trainer shouts at the wiry men, who have barely slept in days, as they do situps and other exercises on the rough concrete floor, some fading in and out of consciousness from fatigue. Blasts of cold water from a hose bring them to their senses.

Entry into the Taiwan Navy's elite Amphibious Reconnaissance and Patrol (ARP) unit — its answer to the United States Navy SEALs or the United Kingdom's Special Boat Service — is not for the faint of heart. In the event of war with the People's Republic of China, which claims the democratic island as its own and has stepped up its military and political pressure against Taiwan, ARP frogmen could find themselves spirited across the strait in small boats under cover of night to scout enemy locations and call in attacks.

Of the 31 Marines who started the 10-week course, only 15 finished, with the closing week at the sprawling Zuoying Navy Base in southern Taiwan as the last test.

"I'm not scared of death," Fu Yu, 30, said after completing the "road to heaven," a final obstacle course consisting of a 100-meter-long stretch of rocks over which trainees must scramble and do tasks such as pushups to the satisfaction of their trainers.

"It's a Soldier's responsibility, what we must do," added Fu, who had previously failed to complete the course.

Over six days and five nights, the volunteers to enter the ARP have to endure everything from long marches to hours in the water, with constant screaming by their instructors. A lot of their time is spent in the sea or swimming pools, learning how to hold their breath for extended periods, swimming in full combat gear and infiltrating beaches.

Every six hours they have a one-hour break. In that time, they have to eat — scarfing down bulbs of garlic to boost their immune systems — get medical attention, go to the toilet and sleep. They may only sleep for five minutes, huddled on the floor under light green blankets, awakened with shrill whistle blasts. The aim is to push the Marines to develop an iron will to complete their mission no matter how difficult and to develop steadfast loyalty to their comrades and the military.

The candidates are all volunteers, driven to join the special forces out of patriotism and a desire to push their personal limits. Wu Yu-wei, 26, said he considered it a personal challenge to complete the course. "The hardest part was the timing, not being able to rest, having only 15 minutes to use the toilet, have a gulp of water, before moving on to the next section," he said. "The first few days are exhausting, and then you get used to it. You have to rely on your will power and determination."

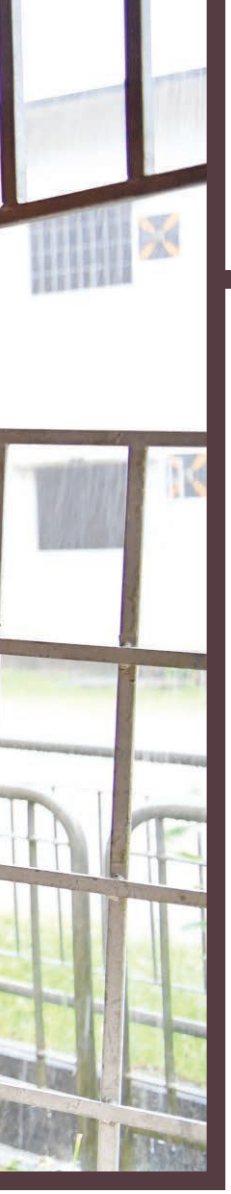
Once across the road to heaven and congratulated by Marine Corps Commander Wang Jui-lin, the stress of the past week is too much for some Marines, who burst into tears in the arms of proud family members invited to see them graduate.

The trainers, all graduates of the course, say the intention of the week of hell is not cruelty but to simulate the hardships of war, such as extreme sleep deprivation, to see who has the stamina and guts to make it.

"Of course, we absolutely won't force anyone. Everyone is here voluntarily. That's why we are so severe with them and also eliminate them strictly," said trainer Chen Shou-lih, 26. "We won't just wave you through only because you wanted to come."

Taiwan Navy Amphibious Reconnaissance and Patrol trainees battle the waves while completing exercises during the 10-week program to join the elite unit.

EMBRACING AN *Evolving Security* ENVIRONMENT



SINGAPORE MINISTRY OF DEFENCE

HENG CHEE HOW/SINGAPORE MINISTRY OF DEFENCE

The Asia-Pacific Programme for Senior Military Officers (APPSMO) was established in 1999 by then-President S.R. Nathan of Singapore. He envisioned a "summer camp" to bring together military officers from across the Asia-Pacific and beyond to discuss defense and security issues in a frank and open manner and to forge relationships. The idea then, as now, is that an informal setting such as APPSMO would be the most valuable opportunity for officers to get to know their counterparts and benefit from the candid discussions that might not be possible during official meetings.

Over the past two decades, APPSMO has developed into an established feature in the regional calendar. The program has brought together experts, practitioners and participants from over 30 countries around the world, including Europe and the Middle East. Such inclusive platforms for military officers to exchange views have become more essential as we confront the numerous security challenges in this period of geopolitical flux.

GEOPOLITICAL TRENDS AND CHALLENGES

Three trends in the evolving security environment are particularly pertinent.

The first is great power competition. In recent years, the United States-China rivalry has intensified. Antagonism between the two countries now covers several areas beyond defense, including trade, technology and finance. One particular domain in which the U.S. and China are competing for leadership is technology. In our region, we are also witnessing the emergence, or reemergence, of regional partnerships, including the Quadrilateral Security Dialogue, or Quad, and more recently, a trilateral security pact involving Australia, the United Kingdom and the U.S. As these initiatives develop, we hope that they will contribute constructively to the peace and stability of the region and complement the regional security architecture.

The second trend is new, nontraditional security challenges that have emerged. The ongoing COVID-19 pandemic is a prime example and climate change is another. Many countries were unprepared to deal with the COVID-19 challenge, and the cost of getting caught unprepared again will indeed be great for any nontraditional challenges yet to emerge.

The third is the disruption and increasing security risks brought by technology and changes in technology. While technological advances have given rise to new opportunities, these have also come with attendant risks. These same technologies have enabled threat actors to exploit vulnerabilities with greater ease and at a lower cost.

The three trends have one thing in common, and that is a strong nexus between technology and security. Technology is a battlefield in great power competition. But it also offers the means to address the challenges of a pandemic and climate change. It brings both enormous opportunities and risks.

NEED FOR MILITARIES TO ADAPT

With the onslaught of the pandemic, the pace of digitalization has accelerated, making societies and countries more vulnerable to threats in this domain. We have become even more dependent on technology, and as our dependency grows, new challenges will surface. All militaries will need to adapt to respond effectively. So, what can militaries do? I propose three lines of effort.

First, armed forces should rethink traditional concepts of defense. In conventional warfare, there are constants that we often take for granted: a clearly identified adversary, an accountable chain of command and defined objectives, just to name a few. Against novel threats in domains such as cyber and information, these constants are not the same. For example, when faced with attacks from the cyber or information domains, how can we be sure of the perpetrator? How do we differentiate between a criminal attack and an attack from a hostile political actor? Then, how do we respond, and who should respond? I believe militaries will need to review their doctrines, structures and capabilities to be able to respond effectively to these threats in this changed environment.

In other emerging areas such as autonomous systems, biotechnology and artificial intelligence (AI), militaries will need to confront questions on ethics and legality. For instance, while AI can act as a force multiplier, there can also be serious consequences if AI behaves in an unanticipated manner. In light of this, Singapore established preliminary guiding principles of responsible, safe, reliable and robust in the defense sector to promote and advance the development and use of AI.

Second, there needs to be greater cooperation between the public and private sectors to enable effective national responses. Upending our traditional conceptions of warfare, today's conflicts often circumvent geographical borders and take place outside the bounds of clear battlefields. Aggressors exploit soft targets, which are less readily defended. Threat actors have used social media to spread false information, embark on influence campaigns and polarize and tear apart societies. Multiethnic and multireligious societies such as Singapore are particularly vulnerable.

It is for this reason that Singapore takes a national approach to cybersecurity strategy. The Cyber Security Agency of Singapore, supported by homefront and defense agencies, works closely with the private sector to protect networks and critical information infrastructures.

Public-private partnerships can also help defense and military establishments leverage opportunities afforded by technology to become more capable and effective. Doing so would enable defense establishments to grow their talent pools, cross-share ideas and innovate, as well as optimize resources to tackle collective challenges to the economy and society.

MULTILATERAL COOPERATION

Third, given the transnational nature of these emerging threats, greater multilateral cooperation will be key to dealing with them effectively. In support of civilian agencies, defense establishments could work together to foster common rules, norms and principles in cyber, information, AI and other emerging domains. In the defense sector, militaries are well-positioned

Senior Minister of State for Defence Heng Chee How views a flight training simulator at the Republic of Singapore Air Force Unmanned Aerial Vehicle Command.
SINGAPORE MINISTRY OF DEFENCE

Singaporean, Thai and U.S. Soldiers spread concrete at a Thai school during a Cobra Gold exercise.
PETTY OFFICER 1ST CLASS JULIO RIVERA/U.S. NAVY

to leverage existing relationships and networks with international partners to tackle transnational security challenges. We therefore encourage our partners in the region and beyond to fully leverage platforms such as the ASEAN [Association of Southeast Asian Nations] Defence Ministers' Meeting (ADMM)-Plus and the Experts' Working Groups.

Singapore has always been a strong advocate for multilateral cooperation to promote regional peace and prosperity, in line with our interest to promote an open and rules-based order. We continue to build on existing networks to enhance practical military cooperation in key domains. In this vein, and as a timely response to the threats in the cyber and information domains, we announced in 2021 that Singapore would establish the ADMM Cybersecurity and Information Centre of Excellence. The center will promote information sharing and research to help the region develop a deeper shared understanding of cyber malware, misinformation and disinformation threats that have implications for defense. Moving forward, it is important for all defense establishments to build on this strong foundation of practical cooperation within the region and explore opportunities to collaborate in new and emerging domains.

FOSTERING FRIENDSHIPS

Today, there are more reasons than ever for countries to work together to tackle common threats. I also hope that armed forces will consider ways to adapt and respond to the widening range of security challenges.

Countries, like friends, may share common interests and perspectives. At the same time, they may not always agree with each other on issues, particularly when conflicting national interests are at stake. The peaceful resolution of disputes requires leaders who are open and willing to talk through differences. This is where strong relationships that you build with your counterparts — a familiar voice at the other end of the phone or, in our current context, a familiar face on the other side of the screen — can make a huge difference.

This is the long-term value of APPSMO: to bolster our regional security architecture by fostering friendships and cooperation among military officers. □

Singapore Senior Minister of State for Defence Heng Chee How delivered this speech in October 2021 during the 22nd Asia-Pacific Programme for Senior Military Officers, held virtually by Singapore's S. Rajaratnam School of International Studies. It has been edited to fit FORUM's format.

TAIWAN INTEGRATES LESSONS OF UKRAINE INVASION IN ANNUAL MILITARY DRILLS


THE ASSOCIATED PRESS

REUTERS

Taiwan incorporated lessons learned from Russia's invasion of Ukraine into upcoming military exercises aimed at practicing fighting off a Chinese attack, according to the self-governed island's National Defense Ministry.

Taiwan, claimed by the People's Republic of China (PRC) as its territory, raised its alert level after the Russian invasion of Ukraine in February 2022, wary that the Chinese Communist Party (CCP) might make a similar move against the island.

Debates have emerged in Taiwan and discussions commenced with the United States on how the island could defend itself, according to Taiwan Defense Minister Chiu Kuo-cheng. "It is not only discussed in exchange meetings between the United States and Taiwan, but also discussed with other countries that have regular contacts with Taiwan," Chiu said in late March 2022.

The Defense Ministry said the Han Kuang exercises, Taiwan's largest annual war games, would be held in two parts in May and July 2022. The first included a tabletop exercise based on "possible actions of the Chinese Communist Party in recent years to invade Taiwan, taking into account the lessons of the Russian-Ukrainian war," according to a ministry statement. The July portion featured five days of drills, including live-fire exercises.

Troops focused on attacking the enemy at sea, preserving combat forces and "integrating the total force of the whole people to support military operations," a reference to civil defense and reservist reforms to improve Taiwan's ability to fight the CCP. (Pictured: Taiwan armored units conduct a live-fire drill during the 2021 Han Kuang exercise on an island in Penghu.)

"The Taiwanese government and people also face a high threat from the authoritarian regime across the Taiwan Strait, and therefore feel the current situation faced by Ukraine as though it is happening to ourselves," Taiwan Foreign Minister Joseph Wu told Vitali Klitschko, mayor of Ukraine's capital, Kyiv, during an April 2022 video conference. Wu pledged Taiwan would donate U.S. $8 million to Kyiv and Ukrainian medical institutions.

Taiwan has condemned Russia's invasion, joined Western-led sanctions and donated U.S. $20 million for Ukrainian refugees, mostly raised from the public. The PRC has not condemned Russia and only donated U.S. $2.3 million in humanitarian aid.

While Taiwan officials see many parallels in the Ukraine war, including having a giant neighbor with territorial ambitions, they have also pointed to major differences. Taiwan, for example, has the "natural barrier" of the Taiwan Strait, which would make it more difficult for the CCP to land troops. Taiwan also has a large and well-equipped Air Force and is developing a formidable missile strike capability.

The CCP has stepped up its military pressure against Taiwan over the past two years. Taiwan rejects the PRC's sovereignty claims and says only the island's people can decide their future.

smoke SHOW

The Royal Australian Air Force Roulettes thrill the crowd before the Australian Formula 1 Grand Prix in April 2022 in Melbourne. Established in 1970, the aerobatics team flies as low as 80 meters and at speeds of up to 685 kilometers per hour. Pilots often pull 6Gs during maneuvers that showcase their judgment and hand-eye coordination.

Photo By: Michael Currie/Royal Australian Air Force

RELEVANT. REVEALING. ONLINE.

www.ipdefenseforum.com

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

FREE MAGAZINE SUBSCRIPTION

FOR A FREE MAGAZINE SUBSCRIPTION:

www.ipdefenseforum.com/subscribe

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

PLEASE INCLUDE:

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

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

All platforms may not be available at every location.