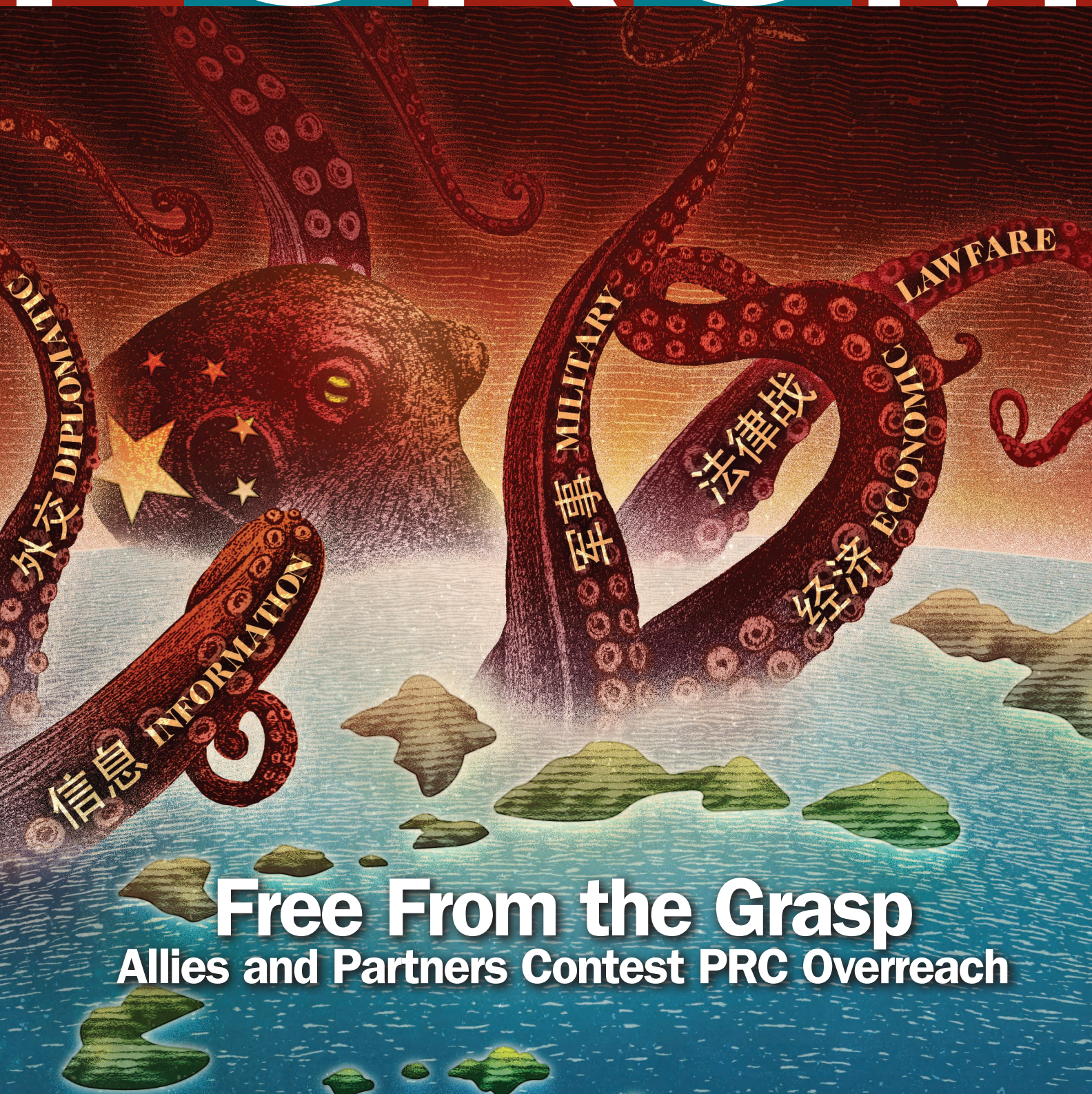


# FORUM



## Free From the Grasp

Allies and Partners Contest PRC Overreach

Compounding Security Risks



# features

## 8 **Space Threats**

An analysis of counterspace capabilities, developments and policies.

## 16 **Road Map for a Global Communist Empire**

From resisting to rewriting the international order, the Chinese Communist Party desires hegemony despite denials.

## 22 **Stepping Up in the Pacific**

Allies and partners bolster Pacific island nations against array of security threats.

## 28 **Black Market Foreign Exchange**

Chinese Communist Party members move money in plain sight, threatening security.

## 32 **The Strategic Spread of Disinformation**

How the CCP has weaponized the information environment and how to compete.

## 36 **Economic Conflict With China**

Meeting the threat together.

## 44 **Russia's Shadow Soldiers**

The Wagner Group gives Putin foreign influence with deniability and his crony a boost in business.

## 50 **Battling Human Trafficking in the Bay of Bengal**

BIMSTEC countries commit to fight exploitation of women and children.

## 56 **Integrating Human Rights Into Peacekeeping**

U.N. promotes readiness in key areas to bolster operations.





# departments

## 4 Indo-Pacific View

## 5 Contributors

## 6 Across the Region

News from the Indo-Pacific.

## 62 Voice

The inaugural Quad leaders summit delivered a clear message to Beijing.

## 66 Contemplations

China's new maritime law creates a means to expand territory through coercion.

## 67 Parting Shot



### ABOUT THE COVER:

This illustration conveys the importance of allies and partner nations working together to counter aggression by the People's Republic of China to maintain a Free and Open Indo-Pacific.

FORUM ILLUSTRATION



Dear Readers,

Welcome to Indo-Pacific Defense FORUM's issue on compounding security risks.

The 21st century has brought nations close to one another in a globalized manner. Combined with rapid disruptive changes, this environment has blurred the boundaries of traditional security threats. This edition analyzes the challenges these threats present to the international rules-based order and how they will affect the Indo-Pacific.

Compounding security risks alter the dynamics of threats and competition. To combat and mitigate these risks, our allies and partners must understand the cultural, economic, and political nuances of the geopolitical landscape.

This edition opens with an analysis of counterspace capabilities, developments, and policies across the region. Although some of our adversaries have made advancements in counterspace weapons, our allies and partners are making innovative progress to counter these developments. As analysts from the Center for Strategic and International Studies detail, Japan and South Korea are evolving their technologies to ensure we maintain superiority. Such advancements require new protocols to protect the space domain and outline norms of behavior in its realm.

Pacific island nations and territories face new security threats, including the proliferation of transnational crime, illegal fishing, and more damaging natural disasters. A feature article highlights the work of the U.S. Army's Operations in Pacific Island Countries that collaborated successfully throughout the region to reduce these security risks.

Dr. Jinghao Zhou of Hobart and William Smith Colleges in New York argues that recent activities by the Chinese Communist Party (CCP) indicate a desire for increased power on the world stage. The CCP's military buildup, wolf-warrior diplomacy, aggressive political propaganda, ideological censorship, and coercive economic policies support this viewpoint. A series of related articles show that our ally and partner network is necessary to counter this aggression.

Dr. Shale Horowitz of the University of Wisconsin-Milwaukee offers regional solutions to mitigate China's economic threats, which often compound the CCP's military-security ones. John F. Tobon of U.S. Homeland Security Investigations reveals the security implications for the Indo-Pacific of the PRC's involvement in black-market foreign exchange. Doowan Lee, CEO and co-founder of an artificial intelligence startup, explains how our ally and partner network can compete against the CCP's digital strategy, which has weaponized the information environment.

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

All the best,

**FORUM Staff**

## IPD FORUM

### Compounding Security Risks

Volume 47, Issue 1, 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](http://ipdefenseforum.com)

email:

[ipdf@ipdefenseforum.com](mailto: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)



**TODD HARRISON** is director of defense budget analysis and director of the Aerospace Security Project at the Center for Strategic and International Studies (CSIS). As a senior fellow in the International Security Program, he leads CSIS's efforts to provide in-depth, nonpartisan research and analysis of defense funding, space security and air power issues.

**KAITLYN JOHNSON** is deputy director and a fellow of the Aerospace Security Project at CSIS. She manages the team's strategic planning and research agenda. Her research specializes in topics such as space security, military space systems, commercial space policy and U.S. air dominance.

**LT. COL. JOE MOYE** is an active-duty U.S. Marine Corps officer with 22 years of service. His operational assignments include a marine expeditionary unit and six deployments to Africa, Europe and the Middle East. His most recent operational assignment was battalion command at Camp Lejeune, North Carolina.

**MAKENA YOUNG** is a research associate with the Aerospace Security Project at CSIS. Her research interests include international collaboration, space security and orbital debris. She has worked for the Federal Aviation Administration as an aerospace engineer, focusing on automatic dependent surveillance-broadcast certification and integration in small aircraft.

Featured on Page 8



**DR. JINGHAO ZHOU** is an associate professor of Asian studies at Hobart and William Smith Colleges in New York. His research focuses on Chinese ideology, politics and religions and U.S.-China relations. He has published dozens of journal and news articles and has written four books, including "Chinese vs. Western Perspectives: Understanding Contemporary China." Featured on Page 16



**JOHN F. TOBON** of U.S. Homeland Security Investigations has over 20 years' experience investigating complex money laundering schemes. He has helped shape international anti-money-laundering policy as a member of U.S. delegations to intergovernmental bodies, including the Financial Action Task Force. Tobon is also an adjunct professor at Florida International University's School of International and Public Affairs, where he lectures on global financial crimes. Featured on Page 28



**DOOWAN LEE** is CEO and co-founder of the artificial intelligence startup VAST-OSINT. He builds data analytics tools that expose and analyze the origin of disinformation and adversarial information operations by using cyber data to authenticate content. He is also a senior advisor to the Institute for Security and Technology and an adjunct professor of politics at the University of San Francisco. Featured on Page 32



**DR. SHALE HOROWITZ** is a professor in the Department of Political Science at the University of Wisconsin-Milwaukee. His research has examined international and ethnic conflict, with an emphasis on East and South Asia; the politics of international trade and finance; and the politics of market transition and institutional change in post-communist countries and East Asia. He has conducted research in China, India, South Korea, Taiwan and countries in Eastern Europe and the former Soviet Union. Featured on Page 36



**ANASUA BASU RAY CHAUDHURY** is a senior fellow with the Observer Research Foundation's Neighbourhood Initiative. She specializes in South Asia, energy politics, forced migration and women in conflict zones. She is editor of the Indian Association for Asian and Pacific Studies' online journal IAAPS Perspective and a regular contributor to peer-reviewed journals, newspapers and magazines. Featured on Page 50

## Join the Discussion

### WE WANT TO HEAR FROM YOU!

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

Indo-Pacific Defense FORUM offers extensive content online, with new articles posted daily at [www.ipdefenseforum.com](http://www.ipdefenseforum.com)

Visitors can:

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



## DOWNLOAD OUR APP!



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



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



Chinese women in Beijing train to be nannies. GETTY IMAGES

# PERMISSION TO PROCREATE

**C**hina now allows married couples to have up to three children, a major policy shift from the existing limit of two after data showed a dramatic decline in births in the world's most populous country.

The change was approved during a May 2021 meeting chaired by Chinese Communist Party (CCP) General Secretary Xi Jinping, the official news agency Xinhua reported.

In 2016, China scrapped its decades-old one-child policy — initially imposed to halt a population explosion — in favor of a two-child limit, which failed to bring a sustained surge in births because the high cost

of raising children in Chinese cities deterred many couples from starting families.

“To further optimize the birth policy, [China] will implement a one-married-couple-can-have-three-children policy,” Xinhua reported.

The policy change comes with “supportive measures, which will be conducive to improving our country's population structure, fulfilling the country's strategy of actively coping with an aging population and maintaining the advantage, endowment of human resources,” Xinhua said. It did not specify the support measures.

The announcement drew a chilly

response on Chinese social media, where many said they could not afford to have even one or two children.

“I am willing to have three children if you give me 5 million yuan [U.S. \$785,650],” one user posted on Weibo. China's latest census showed that the population grew at its slowest rate since the 1950s during the past decade, topping 1.41 billion.

Data also showed a fertility rate of just 1.3 children per woman for 2020, on par with aging societies such as Japan and Italy. The CCP also said it would phase in delays in the country's retirement ages but did not provide details. Reuters

## HISTORIC DRUG *interdiction*

**A**ustralian police said in June 2021 that they foiled a plan to bring nearly 3 tons of cocaine into the country, the largest drug interdiction in the nation's history.

New South Wales State Police Commander Stuart Smith told reporters that officers arrested three men for their roles in a conspiracy to bring drugs into the country. He said the amount was equal to the total amount of cocaine consumed in New South Wales in a year.

Smith said authorities were tipped off to the criminal enterprise in early 2020, when detectives witnessed a man gambling a large sum of money in a casino. That led to an investigation, which revealed an international syndicate operating on four continents.

Smith said the United States Drug Enforcement Administration, acting on information from his agency, intercepted 870 kilograms of cocaine as it was being transported off the coast of Colombia in October 2020.

In April 2020, the U.S. Coast Guard intercepted a boat off the coast of Ecuador carrying 900 kilograms of cocaine.

Smith said the operation culminated in June 2021 with the arrest of the three suspects in Newcastle, New South Wales. They were charged with conspiracy to supply prohibited drugs.

Voice of America News



# STRENGTHENING SECURITY TIES

Japan and Australia share concerns about the People's Republic of China's (PRC's) increasingly assertive actions in regional seas and expressed strong objections to "coercive or destabilizing" behavior.

Foreign and defense ministers from the two countries agreed in June 2021 to strengthen their security ties as the PRC presses its claims to contested areas in the Indo-Pacific region.

Japanese Foreign Minister Toshimitsu Motegi, pictured at right, told reporters that the officials shared their concerns about Chinese activity in the East and South China seas as a challenge to the international community. Motegi was joined by Japanese Defense Minister Nobuo Kishi and their Australian counterparts, Marise Payne and Peter Dutton.

Japan regularly protests to the Chinese government over its coast guard presence near the Japanese-administered Senkaku Islands, which China also claims and calls Diaoyu. Chinese vessels routinely violate Japanese territorial waters around the islands, sometimes threatening fishing boats, Japanese officials say.

Japan and the PRC also disagree on the development of undersea resources in the area.

"We reinforce our strong opposition to any destabilizing or coercive unilateral actions that could alter the status quo and increase tension in the East China Sea," Japan and Australia

said in a statement released after the talks. The behavior "undermines the rules-based international order."

In the South China Sea, the PRC's sweeping maritime claims have clashed with those of its neighbors, which accuse Beijing of militarizing one of the world's busiest sea lanes.

The joint statement expressed "serious concerns about the recent negative developments and serious incidents in the South China Sea, including continuing militarization of disputed features, dangerous use of coast guard vessels and 'maritime militia,' and efforts to disrupt other countries' resources exploitation activities."

"We reaffirmed our strong opposition to any unilateral attempts to change the status quo" by the PRC, Motegi said. He added that the four ministers shared "grave concern" over the PRC's human rights abuses in Hong Kong and the western Xinjiang region, home to Uyghurs and other Muslim minorities.

The statement called on the PRC "to grant urgent, meaningful and unfettered access to Xinjiang for independent international observers including the U.N. [United Nations] high commissioner for human rights."

The meeting also reaffirmed the importance of maintaining peace and stability in the Taiwan Strait, where the PRC has stepped up a campaign of pressure on the self-ruled island of Taiwan. Reuters

## AUSTRALIA/JAPAN



## INDO-PACIFIC



## PRO-DEMOCRACY EMOJI MARKS ANNIVERSARY

Twitter launched an emoji in April 2021 to spotlight the first anniversary of the #MilkTeaAlliance online protest movement that has forged links among pro-democracy activists across the Indo-Pacific.

The alliance — named for the shared love of sweet tea drinks across Hong Kong, Thailand and Taiwan — emerged in 2020 as an expression of cross-border solidarity and shared fear of authoritarian China.

The campaign gained steam at a time when Hong Kong was emerging from months of pro-democracy protests and young activists in Bangkok and other Thai cities were beginning to demand reform of the country's military-drafted constitution and other rights.

It has since spread to Myanmar — where tea with condensed milk is a staple breakfast accompaniment — after a military coup ousted the country's civilian leader Aung San Suu Kyi in February 2021, sparking a mass uprising.

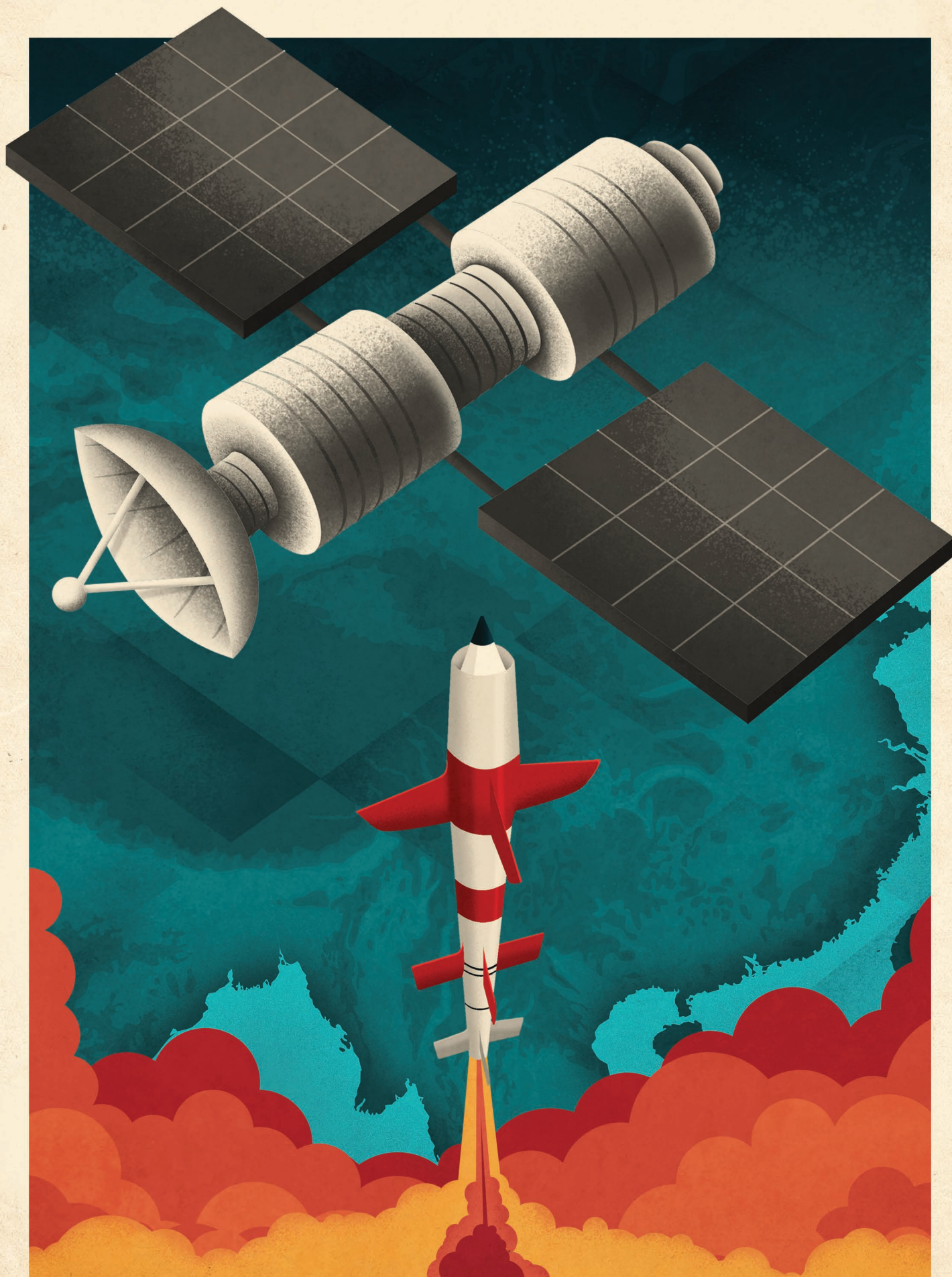
"To celebrate the first anniversary of the #MilkTeaAlliance, we designed an emoji featuring 3 different types of milk tea colors from regions where the Alliance first formed online," Twitter said.

The image appeared in any tweet featuring the hashtag in English, Thai, Korean and several other Asian languages.

"Always in solidarity, no matter how hard the times," veteran Hong Kong pro-democracy activist Joshua Wong tweeted in response to the news, using the English and Chinese versions of the hashtag.

The term has been used on Twitter more than 11 million times since April 2020, the platform said, with usage again spiking after the coup in Myanmar. Agence France-Presse







# SPACE THREATS

---

## AN ANALYSIS OF COUNTERSPACE CAPABILITIES, DEVELOPMENTS AND POLICIES

TODD HARRISON, KAITLYN JOHNSON, LT. COL. JOE MOYE AND MAKENA YOUNG/CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES

---

**T**he year 2020 proved to be one of uncertainty and unpredictability driven by the COVID-19 pandemic, the ensuing global recession and political change in the United States and elsewhere in the Indo-Pacific. For space security, however, 2020 was largely a year of continuity and predictability. The most notable change in the space environment was the addition of some 900 SpaceX Starlink satellites to low Earth orbit (LEO), bringing the total constellation size to more than 1,200. This is the largest satellite constellation in history, and it already makes up roughly one-third of all operating satellites in space. SpaceX continues to build out its constellation, with launches of 60 Starlink satellites at a time every few weeks.

Several notable developments in U.S. space policy also occurred during the previous U.S. administration, under then-President Donald Trump, which issued three new space policy directives (SPDs). SPD-5 directed government departments and agencies to develop cybersecurity policies and practices to improve the protection of government and commercial space assets from cyberattacks. SPD-6 updated national policy for the development and use of space nuclear power and propulsion, and SPD-7 updated policy and guidance for space-based positioning, navigation and timing programs and activities. NASA also unveiled the Artemis Accords in 2020, which include 10 principles with which nations must abide to be part of the Artemis program, a plan to return astronauts to the moon and, eventually, send them to Mars. By mid-2021, 12 nations had signed the accords, including Indo-Pacific nations Australia, Japan, New

Zealand, South Korea and the U.S.

The stand-up of the U.S. Space Force and U.S. Space Command continued throughout 2020 and 2021. The U.S. Space Force submitted its first budget request, for U.S. \$15.4 billion, including U.S. \$15.3 billion transferred from existing U.S. Air Force accounts. It also published its first capstone document, “Spacepower Doctrine for Space Forces,” which was more notable for its continuity with current policy and doctrine than for any significant changes. U.S. Army Gen. James Dickinson, commander of U.S. Space Command, issued his strategic vision in February 2021 to develop a warfighting mindset throughout the command, maintain key relationships with allies and partners, and improve integration across the U.S. government and with commercial space organizations.

Throughout 2020, other nations continued development and testing of counterspace weapons. Most notably, Russia conducted several anti-satellite (ASAT) tests, including a co-orbital ASAT weapon in July 2020 and a direct-ascent ASAT weapon in December 2020. These activities reflect a pattern of behavior in which Russia has continued to develop and reconstitute its counterspace capabilities.

While China, India, North Korea and Russia have the most public advancements in counterspace weapons, other states are developing counterspace capabilities. Japan continues to advance its civil and military space operations. Before passage of its Basic Space Law, Japan prohibited the use of space for national defense. The 2008 law permitted the country to begin military developments



in space, and government officials are speaking about developing defensive counterspace capabilities, largely in response to actions by China in space, such as the 2007 debris-producing ASAT test.

In 2020, Japan authorized a bill to set up its proposed Space Domain Mission Unit within the Japan Air Self-Defense Force to be operational by 2023, with plans to launch the first satellite for monitoring the space environment by 2026. Japan established the Space Operations Squadron in 2020 as the first space domain mission unit with the official mission to protect Japanese satellites from damage, including armed attacks, and to monitor the space environment, including space debris, asteroids and other satellites. The Space Operations Squadron will cooperate with the U.S. Space Command and Japan's civil agency, the Japan Aerospace Exploration Agency. "Japan's security space activities are premised on cooperation with the United States," said Yasuhito Fukushima, a senior research fellow at the Japanese National Institute for Defense Studies.

Japan has not demonstrated any direct-ascent ASAT systems, although it has U.S.-made SM-3 missile defense interceptors with a latent ability to attack space assets in LEO. Because military developments in space are relatively new to the country, most public remarks have been about the possibility of pursuing such capabilities as co-orbital ASAT and jamming technologies. In 2020, then-Prime Minister Shinzo Abe declared that Japan will "drastically bolster capability and systems in order to secure superiority," though no specific programs have been made public.

In South Korea, the government in an October 2020 blog discussed its need to reinforce satellite navigation with terrestrial systems to combat jamming and spoofing. The country cited troubles with spoofing from North Korea, specifically from 2010-16, as a driving force to augment GPS with terrestrial systems. South Korea's Ministry of Science also released a statement detailing plans to upgrade space capabilities, including launching the first locally built rocket to carry satellites and orbiter probes to the moon, with aims for a more powerful rocket by 2029.

## CHINA'S SPACE PROGRAM

Minimal counterspace weapons developments or tests were identified in open-source information during 2020. However, China has a robust direct-ascent ASAT program, dual-use capabilities on orbit that are necessary for co-orbital ASAT weapons and widely used electronic and cyber counterspace capabilities.

Despite the pandemic, 2020 saw accomplishments for China in civil space missions. The Chang'e-5 moon mission returned 2 kilograms of rocks in December 2020. The Yutu-2 rover was still operating on the far side of the moon as of mid-2021 and had traveled over 600 meters on the lunar surface. China also launched the core section of its national space station in June 2021.

## CHINA'S MILITARY SPACE ORGANIZATION

The organization of space assets and missions within China's People's Liberation Army (PLA) remains unclear. Many space missions, such as space launch and the acquisition and operation of satellites, remain within the Strategic Support Force (SSF). Often presented as the "information domain," the SSF maintains PLA efforts for cyber, electronic and psychological warfare, and space. The Space Systems and Network Systems departments (co-equal semi-independent branches within the SSF) share joint missions, including counterspace capabilities. A Center for the Study of Chinese Military Affairs report notes that "another important principle that appears to have influenced the design of the SSF is the enduring Maoist imperative of peacetime-wartime integration." This principle is well suited for the dual-use nature of many space and counterspace capabilities.

Chinese civil space capabilities, such as the Martian rover, are led by the China National Space Administration, which falls within the purview of the State Council's State Administration for Science, Technology, and Industry for National Defense. The China Aerospace Science and Technology Corp. and the China Aerospace Science and Industry Corp. are two examples of the many research and development arms of the Chinese government that specialize in space technologies.

## CHINESE COUNTERSPACE WEAPONS

China continues to test its operational SC-19 direct-ascent ASAT system, yet it has already demonstrated that its direct-ascent ASAT capabilities can threaten any satellite in LEO and likely in medium Earth orbit and geosynchronous equatorial orbit (GEO) as well.

Tianjin University has developed a robot to support space debris-removal missions. This tentacle-like robotic arm would be placed on satellites and launched into orbit to grapple debris and clear it from popular orbits. The robotic arm could, in theory, be used to grab an adversary's satellite, although it would probably require extremely close rendezvous proximity operations (RPOs) that would not be effective with debris or defunct satellites tumbling uncontrolled in space.

Some analysts have made claims of massive developments in Chinese ground-based laser stations, including the identification of five suspected locations of such programs within China. While some of the programs identified appear to be academic and, therefore, are likely not ASAT systems, one location of primary concern is a military base known for conducting kinetic physical ASAT tests that may also house a laser weapon system. There is no indication of how advanced or "ready to mobilize" such a directed energy system may be, and there has been no publicly available information about potential tests or attacks against space systems.

In late October 2020, the Indian newspaper Hindustan Times accused China of moving mobile jammers within





**U.S. Air Force Airmen transitioning to U.S. Space Force Guardians take an oath at Travis Air Force Base in California.** THE ASSOCIATED PRESS

60 kilometers of the Line of Actual Control in Ladakh, part of the disputed Kashmir region between India, Pakistan and China, to hide PLA movements in the area.

There have been no publicly acknowledged cyberattacks from China against space systems of the U.S. or other nations. However, China has successfully proved this capability and continues to be active with cyberattacks in other domains against financial or defense-related targets.

### **RUSSIA'S MILITARY SPACE CAPABILITIES**

The COVID-19 pandemic slowed most industries in a large portion of countries mentioned in this report, but Russia's military space capabilities kept a steady pace. In 2020, Russia tested numerous counterspace capabilities, performed complex RPOs and expanded its space-based military infrastructure. The country's consistent space launch capability, continuous advance of counterspace capabilities and civil space contributions through the International Space Station have maintained Russia's status as a major space power, and its prowess in the space domain has fostered unique relationships with foreign countries that are sometimes rivals in other domains.

Russia's state-sponsored space activities fall into either the Russian Aerospace Forces (RAF) or the civil

Roscosmos program. Within the Russian military, space capabilities fall under the RAF. A subsection of the RAF is the Russian Space Force, which was created in 1992 as the world's first space force and is responsible for monitoring all space-based assets, military launches and potential threats to space systems.

In 2020, Russian President Vladimir Putin approved a document that empowers him to use nuclear weapons in response to a conventional strike targeting the country's critical government and military infrastructure. In addition to defending against conventional weapons, space-based weapons are mentioned as a threat in the document, which also calls out the potential deployment of missile defense and offensive strike weapons in space as posing a threat to Russia. The approval of this document signals that Russia believes space-to-Earth weapons could pose as much of a threat as nuclear weapons and would elicit the same response from the country.

### **RUSSIAN COUNTERSPACE WEAPONS**

Russia has possessed kinetic physical counterspace capabilities since the Soviet Union's first co-orbital ASAT test in the 1960s. The technology used in Soviet-era programs proved to be solid building blocks for more recent Russian developments, and the country has



# TYPES OF COUNTERSPACE WEAPONS

**S**pace is an increasingly important enabler of economic and military power. The strategic importance of space has led some nations to build arsenals of counterspace weapons to disrupt, degrade or destroy space systems and threaten the ability of other nations to use the space domain. However, the importance of space has also spurred efforts to deter or mitigate conflict and protect the domain for peaceful uses. For example, the U.S. Space Force's capstone publication on space power notes that "military space forces should make every effort to promote responsible norms of behavior that perpetuate space as a safe and open environment" in accordance with international laws and national policies.

Counterspace weapons, particularly those that produce orbital debris, pose a serious risk to the space environment and the ability of all nations to use the space domain for prosperity and security. Counterspace weapons vary significantly in their effects, how they are deployed and the level of technology and resources needed to develop and field them. They can be categorized into four broad groups of capabilities: kinetic physical, nonkinetic physical, electronic and cyber.

## KINETIC PHYSICAL

Kinetic physical counterspace weapons attempt to strike directly or detonate a warhead near a satellite or ground station. The three main forms of kinetic physical attack are direct-ascent anti-satellite (ASAT) weapons, co-orbital ASAT weapons and ground station attacks. Direct-ascent ASAT weapons are launched from Earth on a suborbital trajectory to strike a satellite in orbit, while co-orbital ASAT weapons are placed into orbit and maneuvered into or near their target. Attacks on ground stations are targeted at the terrestrial sites responsible for command and control of satellites or the relay of satellite mission data to users.

A kinetic physical attack in space will produce orbital debris, which can indiscriminately affect other satellites in similar orbits. These types of attacks are one of the

only counterspace actions that carry the potential for the loss of life if targeted at crewed ground stations or at satellites in orbits where humans are present, such as the International Space Station in low Earth orbit. No country has conducted a kinetic physical attack against another country's satellite, but China, India, Russia and the United States have successfully tested direct-ascent ASAT weapons.

## NONKINETIC PHYSICAL

Nonkinetic physical counterspace weapons affect satellites or ground systems without making physical contact. Lasers can temporarily dazzle or permanently blind satellite sensors or cause components to overheat. High-powered microwave (HPM) weapons can disrupt a satellite's electronics or cause permanent damage to its electrical circuits and processors. A nuclear device detonated in space can create a high-radiation environment and an electromagnetic pulse (EMP) that would have indiscriminate effects on satellites in affected orbits.

Satellites can be targeted with lasers and HPM weapons from ground- or ship-based sites, airborne platforms or other satellites. A satellite lasing system requires high beam quality, adaptive optics (if being used through the atmosphere) and advanced pointing control to steer the laser beam precisely — technology that is costly and requires a high degree of sophistication. An HPM weapon can be used to disrupt a satellite's electronics, corrupt stored data, cause processors to restart and, at higher power levels, cause permanent damage to electrical circuits and processors.

A nuclear detonation in space would immediately affect satellites within range of its EMP, and it would also create a high-radiation environment that would accelerate the degradation of satellite components over the long term for unshielded satellites in the affected orbital regime. The detonation of nuclear weapons in space is banned under the Partial Test Ban Treaty of 1963, which has more than 100 signatories, although China and North Korea are not among them.

## ELECTRONIC

Electronic counterspace weapons target the electromagnetic spectrum through which space systems transmit and receive data. Jamming devices interfere with the communications to or from satellites by generating noise in the same radio frequency band. An uplink jammer interferes with the signal going from Earth to a satellite, such as the command-and-control uplink. Downlink jammers target the signal from a satellite as it propagates down to users on Earth.

In spoofing, an attacker tricks a receiver into believing a fake signal is the real signal. A spoofer can be used to inject false information into a data stream or to issue false commands to a satellite to disrupt its operations. User terminals with omnidirectional antennas, such as many GPS receivers and satellite phones, have a wider field of view and thus are susceptible to downlink jamming and spoofing from a wider range of angles on the ground.

Through a type of spoofing called “meaconing,” even encrypted military GPS signals can be spoofed. Meaconing does not require cracking the GPS encryption because it merely rebroadcasts a time-delayed copy of the original signal without decrypting it or altering the data. The technology needed to jam and spoof many types of satellite signals is commercially available and inexpensive, making it relatively easy to proliferate among state and nonstate actors.

## CYBER

While electronic forms of attack attempt to interfere with the transmission of radio frequency signals, cyberattacks target the data itself and the systems that use, transmit and control the flow of data. Cyberattacks on satellites can be used to monitor data traffic patterns, intercept data or insert false or corrupted data in a system. These attacks can target ground stations, end-user equipment or the satellites themselves. While cyberattacks require a high degree of understanding of the systems being targeted, they do not necessarily require significant resources to conduct and can be contracted out to private groups or individuals. Even if a state or nonstate actor lacks internal cyber capabilities, it may still pose a cyber threat.

A cyberattack on space systems can result in the loss of data or services being provided by a satellite, which could have systemic effects if used against a system such as GPS. Cyberattacks could have permanent effects if, for example, an adversary seizes control of a satellite through its command-and-control system. The attacker could shut down all communications and permanently damage the satellite by expending its propellant supply or issuing commands that would damage its electronics and sensors.



**This computer graphics image provided by the Japan Aerospace Exploration Agency shows an asteroid and the asteroid explorer Hayabusa2.** THE ASSOCIATED PRESS

repeatedly displayed direct-ascent and co-orbital ASAT capabilities — and tested both in 2020.

In response to a July 2020 test in which Russia’s Cosmos 2543 fired a small projectile near an unrelated Russian satellite, U.S. Space Command condemned the test and asserted that such a projectile could be used to target satellites. In response, the Russian Ministry of Defence said these matryoshka, or nesting, satellites are deployed for routine inspections and surveillance of Russia’s other space assets. The Kremlin has continued to assert that Russia has always been and remains a country committed to fully demilitarizing outer space.

Russia continues to develop its air and missile defense systems. Though not officially designated as ASAT weapons, the S-400 and S-500 series surface-to-air missile (SAM) systems could likely reach a satellite in LEO. Russian military sources claim that the S-500 is designed to strike objects in space and defend against space-based weapons. The head of Russia’s Air and Space Forces has said that the S-500 is capable of destroying hypersonic weapons and satellites in near space. The missile class could be used as a counterspace weapon, according to the deputy chief of the RAF’s SAM troops, Yuri Muravkin. “The boundaries between air and space are being, and will be, erased as the aerial enemy gradually becomes an aerospace one,” he said.

Russia also continues to grow its electronic counterspace capabilities and is developing mobile ground-based systems to interfere with foreign satellites. Its electronic capabilities have been increasing at a steady pace since the early 2000s and accelerated in 2009 with the stand-up of electronic warfare troops within the Russian military. Recent developments in electronic counterspace weapons include the Tirada-2, a mobile jamming system “for suppression of space communications,” and the Bylina-MM, a ground-based mobile system focused on jamming satellite communication channels. Bylina has been reported as “a series of ground-based mobile automated stations” and a mobile command-and-



Astronauts salute before boarding China's Shenzhou-12 spacecraft on a Long March-2F carrier rocket at the Jiuquan Satellite Launch Centre in China in June 2021.

AFP/GETTY IMAGES



control system with artificial intelligence. It includes an automated system that is able to recognize assets and determine how to attack them, and it can be used against a variety of ground-, air- and space-based targets. Russia also reportedly has two radar jammers, Krasukha-2 and Krasukha-4, which may be capable of interfering with radar reconnaissance satellites.

## NORTH KOREA'S SPACE PURSUITS

North Korea's counterspace pursuits were subdued in 2020. It remains unlikely that North Korea is capable of or actively pursuing direct-ascent or co-orbital ASAT weapons, and there is little indication that it has advanced its nonkinetic physical capabilities, though some sources insist that a North Korean electromagnetic pulse threat exists. North Korea has demonstrated the ability to conduct electronic warfare through jamming capabilities, and its cyberattack threat is active and viable. These latter two capabilities have the greatest potential for counterspace applications. Claims that North Korea and Iran have resumed cooperation on missile and launch vehicle technology suggest advancement by one nation may be transferable to the other.

North Korea continues to claim peaceful intentions in space, despite a United Nations Security Council report labeling the regime's space program as a threat to international peace. In May 2020, North Korean state television aired a segment on the National Aerospace Development Administration to promote the nation's space program. Pyongyang's propaganda service, Naenara, stated that the purpose of North Korea's space program is to "adhere to the interests of the state and to use science and technology to solve scientific and technological problems essential to economic construction and people's lives." However, much like in the case of Iran, it is widely suspected that North Korea's space intentions are closely tied to its ballistic missile aspirations.

The regime maintains two established launching areas for space capabilities: the Tonghae Satellite Launching Ground and the Sohae Satellite Launching Ground. No

open-source information emerged in 2020 regarding use of the Tonghae site. The website 38 North published imagery and analysis reporting normal maintenance, snow clearing and routine activity, but nothing to indicate the preparation for or execution of a launch in 2020. North Korea also has a General Satellite Control Building (GSCB) intended to track and monitor its own satellite launches and orbiting satellites. Reports indicate the ongoing construction of what is believed to be scientific testing facilities next to the GSCB, though their exact purpose is unclear.

North Korea also does not appear to be pursuing a co-orbital ASAT weapon. To date, the North has not demonstrated the means and expertise to conduct RPOs or active guidance measures required for a viable co-orbital ASAT capability. With only a handful of North Korean objects currently in space, and minimal activity at its two launch facilities, it is unlikely that North Korea is actively pursuing either direct-ascent or co-orbital ASAT capabilities.

When it comes to electronic warfare operations, the North continues to exercise its downlink jamming capabilities. In April 2020, it announced that it was preparing to deploy a new "GPS jamming device" for use against South Korea. There were multiple reports in 2020 that North Korea continues to conduct jamming operations along the Korean Peninsula. Many open-source reports highlight jamming focused on commercial radio broadcast frequencies and civilian GPS signals rather than military targets. The U.S. Army published a new manual titled "North Korean Tactics" in July 2020 that details the North's electronic warfare organizations, capabilities, techniques and tactics.

The greatest North Korean counterspace threat to the U.S. remains a cyberattack, according to U.S. officials. North Korean tactics call out the regime's Cyber Warfare Guidance Unit, known as Bureau 121. The U.S. Army manual describes Bureau 121 as consisting of more than 6,000 members, with many operating in countries such as Belarus, China, India, Malaysia and Russia.

Then-U.S. Secretary of State Mike Pompeo said in December 2020 that North Korea posed a greater threat to U.S. cybersecurity than Russia. This sentiment was echoed by U.S. President Joe Biden's administration in February 2021. North Korea's malicious cyber activities threatening the U.S. and its allies helped to inform a review of U.S. policy, U.S. State Department spokesman Ned Price said.

## INDIA'S GROWTH

Since launching its first satellite in 1980, India has shown progressive growth in its space capabilities. With a successful ASAT test in 2019, India became the fourth country to demonstrate a kinetic counterspace capability. India is also advancing its civil space program, which is working on its third mission to the moon.

India's space activities are bifurcated into civil and military space organizations. All civil space developments fall under the Indian Space Research Organisation, which operates under the Department of Space. The agency celebrated its 51st launch in November 2020, its only launch of 2020, due to the pandemic. India's first orbital launch of 2021 was February 28, when it delivered 19 satellites into orbit, including an Earth observation satellite for Brazil.

In 2019, India created the Defence Space Research Organisation (DSRO), which is charged with the research and development of national security space systems and operates under the Defence Space Agency in the Ministry of Defence. These new agencies are part of India's goal to advance strategic space operations. The DSRO was tasked with developing space warfare systems and technology. Many Indian counterspace capabilities are developed to respond to security threats posed by China and Pakistan.

India has also been working with private companies to provide space domain awareness data to "detect, identify, and track enemy assets." The Defence Space Agency hopes the system, once developed, can play defensive and offensive roles.

## WHAT TO WATCH

While China continues to make progress in developing counterspace weapons, its focus appears to be shifting to integrating these capabilities into its forces and operational plans. A key issue to watch is China's overall investment in space-related research and development and dual-use space capabilities, such as its tentacle space debris cleanup robot. From an operational perspective, a key development to track is the progress China makes integrating its electronic counterspace capabilities, such as jamming and spoofing, into its irregular warfare forces and tactics. In terms of norms of behavior in space, a key indicator to watch is China's Shijian-17 (SJ-17) GEO inspector satellite. While SJ-17 appears to have focused on inspecting other Chinese satellites so far, its possible use to inspect another nation's satellites in GEO would mark an important shift that could have broader repercussions.

Russia is perhaps the most likely nation to conduct additional counterspace testing and deployment over the coming year. Given the tests of its direct ascent and co-orbital ASAT weapons in 2020, a key issue to watch is whether these tests continue and if new capabilities are demonstrated. Other areas to watch for with Russia include tests of laser ASAT systems on additional airborne and ground-based platforms, electronic warfare systems for the protection of critical platforms and emboldened cyberattacks against civilian infrastructure and government institutions.

Both Iran and North Korea continue to have relatively immature space capabilities, but their electronic and cyber counterspace capabilities pose a serious threat. Over the coming year, Iran will likely continue its space launch activities under the Islamic Revolutionary Guard Corps, and North Korea may look to restart testing of its space launch capabilities after a year of relative dormancy. A key development to watch is any additional indication that Iran and North Korea are cooperating in space or ballistic missile technology. Additional issues to watch include continued Iranian GPS spoofing in the Persian Gulf and North Korean GPS jamming into South Korea. An increased frequency and sophistication of cyberattacks by either country in other domains could also indicate a higher level of cyber threats to space systems.

India appears likely to continue development of high-powered lasers and other nonkinetic ASAT capabilities. Key indicators for India in space include how its new military and research and development space agencies continue to develop, the level of funding provided for space and counterspace activities and signs that it is adapting or testing its electronic warfare systems for use against space systems.

Overall, 2020 was a slow year for counterspace activities, with a few notable exceptions. That may change as nations reemerge from lockdown and return to their prior plans and programs. As President Biden's administration develops and refines its overall national security strategy, one of the key areas to watch will be how it addresses space policy issues in general and the proliferation of counterspace weapons. Calls within the U.S. and elsewhere for more clearly defined norms of behavior in space are growing. An early indication that President Biden's administration intends to make progress toward building norms in space would be an agreement among the U.S. Defense Department and the intelligence community for which norms the U.S. government is willing to support and follow. Without an interagency agreement within the U.S. government, it will be difficult to start a meaningful conversation with other governments. □





# ROAD MAP FOR A GLOBAL COMMUNIST EMPIRE

From resisting to rewriting the international order,  
the Chinese Communist Party desires hegemony despite denials

STORY BY DR. JINGHAO ZHOU/HOBART AND WILLIAM SMITH COLLEGES | PHOTOS BY THE ASSOCIATED PRESS

**S**ince the Chinese economy took off in the early 1980s, the Chinese Communist Party (CCP) has repeatedly vowed that the Chinese government will not export its development model and seek global hegemony. In reality, the CCP's fast military buildup, aggressive political propaganda and ideological censorship, along with ambitious economic plans such as its Made in China 2025 and One Belt, One Road (OBOR), indicate that the Chinese government wants to translate the nation's domestic economic power into worldwide dominance toward the establishment of a China-centric global communist empire. The CCP justifies its ambition as "the great rejuvenation of the Chinese nation," or as the China Dream, which CCP General Secretary Xi Jinping has championed since coming into power in 2012 as building a "community of shared future for mankind."

#### **A Potential Terminator of International Institutions**

It is almost impossible for any country to become powerful outside international institutions. China, confronted with the international institutions, suffered tremendously — economically and politically — under international sanctions in the first 26 years of communist control under Mao Zedong. As early as the 1950s, Mao declared that the newly founded People's Republic of China (PRC) would catch up to the United Kingdom in 15 years and surpass the United States in two decades. However, communist China was on the verge of collapse when Mao died in 1976. Under the leadership of Deng Xiaoping, the PRC altered its hostility strategy toward engagement and began to participate in international institutions to fulfill the CCP's global ambitions. Deng's low-profile strategy was designed to buy time and quietly build a communist empire.

China has benefited greatly from international institutions in the post-Mao era, but the CCP is never satisfied with international institutions. The CCP does not simply accept the international order but pragmatically performs as three actors: a potential terminator, a selective participant and a free rider of international organizations. As early as 1996, the book "China Can Say No," written by Chinese nationalists, expressed China's dissatisfaction with the international order, calling on the government to stand up against the U.S. In 2006, a follow-on book by different authors, titled "Unhappy China," articulated China's discontent with the international order and encouraged China to become a hegemon. To incite Chinese nationalism, the

CCP claims that the PRC should obtain what the party wants because Western governments bullied China during the century of humiliation.

In the CCP's view, it is very difficult for China to fulfill the China Dream within the international order because it is built by the U.S. and supported by three systems: U.S. or Western values, the U.S.-led military allies, and the United Nations and its institutions. The CCP's strategy toward international institutions changed from time to time based on its national comprehensive power. As China gradually became strong economically, the PRC began to challenge international institutions in the late 1990s, and it began to shift from Deng's low-profile strategy to an aggressive strategy after China became the world's second-largest economy in 2010. Since the U.S. rejected the Chinese government's proposal of a new type of bilateral great power relationship, the PRC has completed the transition from a hybrid "weak-strong" state strategy to a strong-state strategy, aiming to restore the perceived dominant status in East Asia that Chinese empires enjoyed prior to the 19th century.

Propaganda is central to the Chinese government fulfilling its goal. The CCP wages a global "discourse war" to control external narratives about the PRC because it understands that whoever controls the right to speak controls the international system. The Chinese government established over 1,000 Confucius Institutes around the world to further propaganda at universities and colleges abroad. Chinese foreign-agent spending in the U.S. has increased from U.S. \$10 million in 2016 to U.S. \$64 million in 2020, a fivefold increase to influence U.S. business, political and social climates, according to the Center for Responsive Politics, a nonpartisan research group based in Washington, D.C. The China Screen, a digital billboard in New York City's Times Square, symbolizes the CCP's propaganda in the U.S., displaying CCP ideology 24 hours a day. China Radio International has contracts to broadcast from more than a dozen radio stations in the U.S. alone, while China Daily places inserts in newspapers such as The Washington Post. Beijing has also used other Western media platforms, including Facebook and Twitter, to disseminate propaganda targeting users worldwide. The propaganda targets overseas Chinese and non-Chinese foreigners to create a positive view of the CCP, encourage foreign investment in China, suppress anti-CCP voices and promote anti-American sentiments. The malign influence of the CCP in the U.S. and other free societies is systematic.





**International Monetary and Financial Committee members attend the World Bank/International Monetary Fund annual meetings, often held in Washington, D.C. China is campaigning for a super-sovereign reserve global currency to advance its position in the international financial system.**

### Blurring International Rules

Marshaling all its influence tools, the CCP is challenging the international order by redefining the meaning of international rules. In the security arena, the Communist Chinese government argues that since the end of World War II, nuclear proliferation has been in line with the U.S.-led international order. When democratic countries such as Israel and India seek nuclear weapons, the U.S. has adopted a fuzzy policy, the CCP claims. When countries such as Iran, Iraq, Libya and North Korea seek nuclear weapons, the U.S. has imposed sanctions, the CCP argues in its quest to change the rules and the values on which they are based.

On the issue of climate change, the PRC has repeatedly advocated “common but differentiated responsibilities” at meetings of the International Conference on Climate Change, while Western powers believe that developing and developed countries should bear equal responsibilities. The PRC played a key role in blocking a climate accord at the U.N. Climate Change Conference in Copenhagen, Denmark, in 2009 and made no substantial promises at the virtual 2021 Leaders Summit on Climate. Xi’s promise is empty without any action plan. By contrast, the administration of U.S. President Joe Biden announced an ambitious plan to cut the nation’s emissions 50%-52% by 2030 from 2005 levels.

In the financial sphere, the PRC has firmly advocated separation from international political issues to avoid politicizing economic and financial affairs, attempting to defend authoritarian regimes worldwide. The PRC pushed to obtain the special drawing rights designation for its currency, the renminbi, in 2016 and is advocating for a super-sovereign reserve global currency to advance its position in the international financial system. It has also implemented renminbi settlement pilots internationally to reduce reliance on the U.S. dollar for these transactions. The PRC is introducing a digital currency, which it plans to showcase at the 2022 Winter Olympics in Beijing, in an attempt to assert itself as a global leader in payments technology. The digital version of the renminbi is intended to also create efficiencies in the Chinese economy to challenge the supremacy of the U.S. dollar.

### A Selective Participant and Free Rider

The CCP has used international institutions as platforms to maximize its benefits and expand its global influence. Generally, the Chinese government opposes the political aspect of globalization but supports the economic aspect to reach technological supremacy and export its development model to countries in the Global South and elsewhere. China has used the loopholes of international

institutions to promote unfair trade competition. When China was allowed access to the World Trade Organization in 2001, the Chinese government promised to reform its economic system to meet the organization's requirements but failed to fulfill many of the commitments.

The PRC is predominantly responsible for the theft of U.S. intellectual property. Over 80% of all cases charged as economic espionage involve China, and 60% of all trade secret cases involve China, according to the U.S. Department of Justice. Chinese theft of U.S. intellectual property costs U.S. \$225 billion to U.S. \$600 billion annually. China has been a free rider for decades while the U.S. has had to bear the burden of providing public goods for maintaining international security and prosperity.

The PRC has used vast sums of money from international institutions to promote its domestic and international projects. China borrowed U.S. \$450 million in 1981 and U.S. \$600 million in special drawing rights in 1986 from the International Monetary Fund, received up to U.S. \$9.95 billion in concessional loans from the International Development Association through 1999 and borrowed U.S. \$39.8 billion from the International Bank for Reconstruction and Development through 2011. The PRC now is an upper-middle-income country but still accepts financial assistance from developed countries, including Germany and the U.K. The Chinese government uses the money to buy global power and pressure recipients of Chinese aid to support China or make diplomatic concessions. The World Health Organization (WHO) has provided China with technical assistance worth over U.S. \$100 million, but now the PRC is using its distribution of COVID-19 vaccines to subvert democracy and seek world hegemony.

#### **A Climber in Regional and International Organizations**

The CCP has dramatically increased its role in international institutions by enhancing its power in these agencies. China is a member of more than 200 international organizations and holds the top post in four of the 15 specialized agencies in the U.N., as well as many other senior positions in global organizations. The CCP attempted but failed to gain the top position in the U.N.'s World Intellectual Property Organization two years ago. China has tried to play leading roles in multilateral organizations such as BRICS (Brazil, Russia, India, China and South Africa), the Association of Southeast Asian Nations (ASEAN) and the Asia-Pacific Economic Cooperation.

The PRC has initiated various China-led multilateral organizations, including the China-Arab States Cooperation Forum, the China-Africa Cooperation Forum and the China-ASEAN Free Trade Area. In 2001, China created the Shanghai Cooperation Organisation, a Eurasian political, economic and security alliance. In 2015, China began to promote the Asian Infrastructure Investment Bank and showed a willingness to play a

leadership role to build and maintain the bank. The bank is headquartered in Beijing and has 103 members and 21 prospective members worldwide.

OBOR is the PRC's ambitious project to expand its global influence by transforming the Chinese development model, developing multiple trade relations and establishing a new international trade framework. All these efforts aim to remake regional and global order, driven by the CCP's leadership.



**A worker prepares a display ahead of an auto show in Shanghai. China is responsible for most theft of U.S. intellectual property, including over 80% of all cases charged as economic espionage and 60% of all trade secret cases, according to the U.S. Department of Justice.**

Meanwhile, the Chinese government continues to play hardball in the international political arena. The CCP's values, by nature, are entirely opposed to what are considered universal values and human rights. It has persistently persecuted domestic political and religious activists in the name of giving priority to "collective human rights" and the "right to development," while regularly opposing condemnation of human rights abuses worldwide. The U.N. Human Rights Council has never passed a resolution condemning China's human rights abuses. Whenever such a resolution has been introduced at the council's annual meeting, most member states supported a no-action motion from China or one of its backers.

China has also developed sufficient skills to negotiate in multilateral dialogues by showing gestures of compliance in exchange for other benefits. As a result, China continues to have among the world's worst human rights records and ranked as the biggest jailor of journalists in 2020.

#### **Consequences of China's Threat**

The CCP's goals are multifaceted. It wants to retain the one-party system, unify the so-called greater China — Hong Kong, Macao, the mainland and Taiwan — and turn the South China Sea into its inner lake. It also intends to become the world's superpower. As the first step toward



its ultimate goal, the CCP has developed the concept that “it is for the people of Asia to run the affairs of Asia.” The mantra serves as a justification to build regional primacy as a springboard to global power, destroy U.S. regional alliances and drive the U.S. out of the Indo-Pacific.

China poses serious challenges to U.S. interests, including its economy, values and military. In its 2020 report to Congress, the U.S. Defense Department made clear that the People’s Liberation Army’s objective is to become a world-class military by 2049. A recent Rand Corp. report, titled “China’s Quest for Global Primacy,” predicts that if the U.S. cannot maintain its position as a global leader, it could become a marginalized actor in Asia.



**Chinese Communist Party foreign affairs chief Yang Jiechi, center, speaks at the opening session of the U.S.-China talks in Anchorage, Alaska, in March 2021.**

Most think tanks predict that the Chinese economy will surpass that of the U.S. China will be powerful, and it will seek to drive the world away from democratic values and the rule of law. The coming decade will be critical for both nations and for the global community. Historically, there were great power competitions between the U.S. and the U.K., the U.S. and Russia and the U.S. and Japan. Twenty years ago, Dr. John Mearsheimer, an American political scientist and international relations scholar, noted that great power rivalry was not over. The major powers still fear each other, and dangerous security competition is repeating.

China has been preparing for the battle against the U.S. in three aspects: focusing on domestic priorities and reemphasizing self-reliance policy; reducing dependence on the U.S. while increasing the rest of the world’s dependence on China; and accelerating the expansion of Chinese influence overseas. Xi told CCP members that “the biggest source of chaos in the present-day world is the United States,” essentially identifying the U.S. as China’s enemy.

In March 2021, at the first face-to-face, high-level talks between China and the U.S. under President Biden, the top Chinese diplomatic official attacked U.S. politics

and the U.S.-led international order in an 18-minute diatribe. CCP foreign affairs chief Yang Jiechi insisted that the U.S. does not represent the world, and China will follow its own socialist system because it is better than Western democracy.

Most recently, Xi characterized the development trend of the post-pandemic era as a “rising East and falling West,” saying it was time for China to look the world straight in the eye. In his recent speech published in the CCP’s official journal, *Quishi*, Xi noted that the world is in chaos and that China should seize the opportunity. He claimed that no one can defeat China. Xi has promised to restore China to great power status by 2049. The CCP’s worldview and practices are clear: China totally abandoned Deng’s “low-profile” foreign policy and now is decisively moving in the opposite direction of the U.S.-led international order. At the CCP’s 100th anniversary in July 2021, Xi warned foreign forces that anyone who wants to bully China will have their “heads bashed bloody against a steel wall forged by more than 1.4 billion people.”

### **The Future of Strategic Security Competition**

The future of the global order will largely depend on how the U.S. and the world community respond to China’s comprehensive challenges. There are various misconceptions about China’s threats. Some analysts argue that China has greatly benefited from the current international order and does not intend to overturn it. Others argue that although Beijing has many goals that conflict with those of the U.S., China’s role in international institutions still benefits the global community, including the U.S. There are also those who believe that China’s global influence is limited because China is using its foreign policy principles and approaches to play roles in the international society. Still others argue that U.S. media exaggerate China’s security threat because the international order is complex and multilayered and, therefore, difficult to overturn.

The U.S. National Intelligence Council’s “Global Trends 2040” report envisions five scenarios: The U.S. and its allies will continue to lead the international system; the international order is aimless, chaotic and unstable; democratic societies are becoming increasingly divided; the world is slowly falling into anarchy; and a global coalition, led by the European Union (EU) and China, is emerging.

Without a doubt, the future of U.S.-led international order is still promising.

Although the CCP’s intention to rule the world is decisive, it is likely a dead end because the China Dream mainly represents the CCP’s worldview. Communist ideas and Chinese patriarchal tradition are no longer popular in China or abroad. China’s development relies heavily on U.S. high technology and service, so it’s not easy for China to implement a self-reliance policy in a short time frame. Pursuing democracy and freedom remains the mainstream goal of the globalized world.



**A blur of thousands of protesters march on the streets in Hong Kong in 2019 against an unpopular extradition bill. Communist ideas and Chinese patriarchal tradition are no longer popular in China or worldwide.**

More and more, countries are standing up to China's aggressive expansion. Canada, the EU and the U.K. have coordinated sanctions against China for human rights abuses on minorities. The EU Parliament passed a motion in May 2021 to formally freeze the EU's proposed investment agreement with China and to call on the EU to increase coordination with the U.S. to deal with China. Germany has enacted a supply chain law requiring German companies to limit their activities in or leave the Xinjiang region in northwest China, where the CCP is accused of genocide against ethnic Uyghurs.

More important, the U.S. remains strong. At his first news conference in March 2021, President Biden said that China wants to "become the leading country in the world, the wealthiest country in the world and the most powerful country in the world." He added, however, "That's not going to happen on my watch."

President Biden's administration has been retooling U.S. alliances to strengthen and innovate its international network. The U.S. has rejoined the WHO and the Paris Agreement on climate change, and it is working closely with the EU, NATO and the Group of Seven on issues such as technology, climate change and human rights to counter China's threat.

In the Indo-Pacific after World War II, the U.S. built treaty alliances with Australia, Japan, the Philippines, South Korea and Thailand.

Known as the Quadrilateral Security Dialogue, or Quad, Australia, India, Japan and the U.S. closely cooperate in the economic, military and supply chain arenas. They also conduct multilateral military exercises and are inviting more countries to participate in the Quad, which aims to create a substantial deterrent to the CCP's hegemonic ambitions.

Meanwhile, the Taiwan Strait and the South China Sea have already become the frontier of competition between China and the U.S. and may prove to be the first litmus test of the global community's resolve to block China's path to global hegemony. While the CCP asserts that China's complete reunification is an unshakable commitment of the party, the U.S. no longer sees Taiwan as a problem in its relations with the PRC, but as an opportunity to promote a Free and Open Indo-Pacific. This reflects not only that China-U.S. competition is becoming more intense, but it also demonstrates the decisive determination of the U.S. to continue to maintain its superiority in the Indo-Pacific region. □



# STEPPING UP IN THE PACIFIC

ALLIES AND PARTNERS BOLSTER  
PACIFIC ISLAND NATIONS AGAINST  
ARRAY OF SECURITY THREATS

---

FORUM STAFF

---



**S**cattered across an expanse of ocean that accounts for about 15% of the Earth's surface, the roughly 30,000 Pacific islands — many of them uninhabited atolls — are home to just 12 million people, little more than the population of the Indonesian capital of Jakarta. The livelihoods of many Pacific Islanders are held fast to the riches of their mighty ocean or to the drawing power of their exquisite homelands, tropical jewels atop a shimmering turquoise.

Remote as they may be, Pacific island nations and territories find themselves in the midst of many of the globe's swirling challenges, buffeted by some of the great tests of the era — from rising seas and depleted resources to pandemic lockdowns and geopolitical tussles. "The Pacific region's security environment has become increasingly complex," according to the Pacific Islands Forum (PIF), a political and economic policy group of member states founded in 1971 to foster peace and prosperity through regional and international cooperation. "Pacific communities are vulnerable to security threats from transnational crime groups, climate change, terrorism, natural disasters, political instability and internal conflicts. Consequences include domestic disorder, diminished border revenues, increased local crime and weaker law enforcement."

Above the waves and below the surface, efforts are underway by allies, partners and like-minded nations to fortify the region against a storm of economic, climatic and security threats, including the People's Republic of China's (PRC's) attempts to exert influence for its own gains.

"The Pacific is evolving as complex disruptors intensify and the increasing presence of external actors comes to bear," the New Zealand Defence Force (NZDF) noted in its report "Advancing Pacific Partnerships: A Framework for Defence's Approach to the Pacific," published in October 2019. "Greater competition for influence in the Pacific will intersect with this suite of complex disruptors. External actors seeking to enhance their regional presence may leverage these issues as vectors of influence. More broadly, the pace, intensity and scope of engagement by external actors, who may not always reflect our values across their activities, are at the heart of a growing sense of geostrategic competition that is animating many nations' renewed focus on the Pacific."

## CHINA'S 'EXPANDING ASSERTIVENESS'

Case in point: Kiribati. Among the world's remotest nations, it sits almost midway between Australia and the United States. Although its tiny population of 110,000 could fit comfortably inside India's biggest cricket stadium, Kiribati's 33 coral atolls are sprinkled across an immense sweep of the Pacific, making it the only nation to straddle all four of Earth's hemispheres and giving it an exclusive economic zone (EEZ) of more than 3 million square kilometers — larger than the land area of India. Under the United Nations Convention on the Law of the Sea, Kiribati, like other nations, has sovereign rights to explore and exploit the natural resources within its EEZ. That includes fisheries, oil and gas, and minerals — a trove of resources that has drawn the eye of a rapacious PRC.

In May 2021, Kiribati's government, which dropped its diplomatic ties with democratic Taiwan in favor of communist Beijing in 2019, announced that the PRC was providing financial backing for a feasibility study into upgrading an airstrip on one of the island nation's atolls. The government said the project would support tourism, Reuters reported. Some lawmakers, however, have expressed concern over China's interest in the airstrip, which served as a United States military base in World War II, and questioned whether the project would be part of the PRC's One Belt, One Road, an infrastructure scheme widely panned for its predatory lending practices. A month later, security concerns related to Chinese involvement led to the shelving of a World Bank-led project to install undersea cables to enhance communications on Kiribati and two other Pacific island nations, the Federated States of Micronesia and Nauru. The infrastructure would have linked with an undersea cable that connects with the U.S. territory of Guam and is used mainly by the U.S. government, according to Reuters. A Chinese company submitted the lowest bid, but U.S. and island nation officials warned that Chinese firms are required to cooperate with Beijing's intelligence and security services.

The PRC's involvement in Kiribati's infrastructure projects raises "the prospect of Chinese military bases, or, at least initially, potential dual-use facilities, being established right across the center of the Pacific," noted a September 2020 article in *The Strategist*, a publication of the Australian Strategic Policy Institute, a Canberra-based think tank. "These facilities would give China control over the world's best tuna fishing grounds plus swaths of deep-sea mineral resources, and a presence near the U.S. bases at Hawaii, Kwajalein Atoll, Johnston Atoll and Wake Island. They would also be positioned directly across the major sea lanes between North America and Australia and New Zealand."

---

**The Kiribati patrol vessel RKS Teanoai, left, and United States Coast Guard Cutter Stratton conduct a training exercise in the Pacific Ocean in 2019. The RKS Teanoai was donated to Kiribati as part of an Australian government program that provided patrol boats to 12 Pacific island nations. Australia presented a replacement Guardian-class patrol boat, the RKS Teanoai II, to Kiribati in June 2021.** CHIEF PETTY OFFICER SARA MUIR/U.S. COAST GUARD



# PACIFIC PARTNERS

## BUILDING ENDURING RELATIONSHIPS IN PACIFIC ISLAND NATIONS

OPERATIONS IN PACIFIC ISLAND COUNTRIES

Operations in Pacific Island Countries (OPIC) is a United States Army Pacific-focused effort dedicated to strengthening relationships throughout Oceania. Committed to a Free and Open Indo-Pacific, OPIC reinforces the historical ties of friendship and solidarity between the U.S. and Pacific island nations, including their shared values of personal freedom and global autonomy, embedded with a strong sense of social responsibility. By connecting with military, government and societal partners, the OPIC team uses a vast network of subject-matter expertise to create value across Oceania.

OPIC is composed of Soldiers from all components of the U.S. Army, including active duty, Army Reserve and National Guard. It was officially stood up in 2020, and it mainly includes units and members of the 9th Mission Support Command (9th MSC) located at Fort Shafter Flats, Hawaii, where OPIC is headquartered. With personnel already in Oceania — which includes Melanesia, Micronesia and Polynesia — the 9th MSC is a natural fit for this mission, especially considering its deep ties to the region and that many Soldiers within the mission call Oceania their familial and ancestral home.

“The great thing about the 9th MSC is that in our formations are Soldiers that are actually from [Pacific island] countries,” said U.S. Army Brig. Gen. Timothy D. Connelly, commanding general of the 9th MSC, who took command of OPIC in June 2021. “They are amazing Soldiers with great U.S. Army-acquired military skills and training. They bring to us something that is so unique, and that is the culture and the language and the familiarity of being from, in many cases, the South Pacific.”

As the Oceania effort took shape in early 2020, Oceania Pathways Teams were created to support Pacific island nations. The teams include civil affairs professionals along with cultural experts and are purposely built to accomplish many objectives, with the top two being building host nation capacity and reinforcing relationships across Oceania.

Oceania Pathways Teams have used U.S. Army and sister service engineering, medical and veterinary capabilities to assist throughout the region. The 9th MSC has also sent teams to engage with Pacific island countries for disaster response planning, security cooperation and Soldier skills exchanges. Military-to-military training exercises, such as

Pacific Pathways, increase the readiness of U.S., allied and partner forces. The blending of cultural expertise, civil affairs and the assets that OPIC’s whole-of-government approach brings to the table results in lasting partnerships and sustainable growth.

OPIC has not been without its challenges. Right after the unit launched, the COVID-19 pandemic arrived, dramatically impacting operations. “It forced us to stop everything we were doing and rework our plan moving forward,” said Maj. Eric Morey, who then served as its chief of operations. “From an operations perspective, it was an incredible challenge to figure out. It required a lot of creative solutions, patience and teamwork across all components, allied partners and Oceania countries.”

Despite the obstacles, OPIC moved teams forward to support Pacific island nations. Fiji, the Marshall Islands, Palau, Papua New Guinea and Timor-Leste were the first to benefit from the U.S. Indo-Pacific Command’s (USINDOPACOM’s) increased commitment to Oceania. Supporting the COVID-19 response in these partner nations became a major focus for OPIC.

Though the pandemic presented challenges into 2021, OPIC continued to build capacity and increase its reach to more Pacific island nations. Pivotal to its success has been its ability to provide tailored solutions for each host nation. A key ingredient of that winning formula is the deep cultural affiliation and alignment OPIC has with host nation partners.

Every aspect of its operations includes cultural immersion and education. During a recent physical fitness session, OPIC members took paddling lessons. Led by Master Sgt. Kris Kaopuiki, Soldiers learned the basics of this ancient way of navigating. “There are few better ways to understand, experience and be in touch with the people and cultures that we are helping than paddling,” Kaopuiki said. “The traditions and disciplines of this sport are deeply tied to these ancient societies.” OPIC personnel have also immersed themselves in cultural events, such as kava ceremonies and Pacific Islander heritage nights.

Designed and spearheaded by U.S. Army Pacific, Pacific Pathways seeks to increase the readiness of U.S., allied and partner forces through military-to-military training exercises. The exercises are spread across the Indo-Pacific and have recently included a growing list of Oceania countries.

OPIC entered 2022 as a maturing asset that USINDOPACOM relies upon to continue building strategic relationships and to provide a sustaining presence in the region. From senior leader engagements, joint exercises, conferences, and humanitarian assistance and disaster response planning to COVID-19 support, engineer engagements, and civic actions and projects, OPIC brings an enormous menu of capabilities and value to Pacific island nations. “The U.S. and the Pacific island countries in Oceania share many fundamental values around democracy and a spiritual approach to human existence that embeds respect for the individual within a strong social context,” said U.S. Army Col. Blaise Zandoli, OPIC’s deputy commanding officer. “Our shared values and mutually beneficial practical connections make partnerships a natural outcome.”





Beijing’s “expanding assertiveness” is being felt across the Pacific islands, according to Alexander B. Gray, a senior fellow in national security affairs at the American Foreign Policy Council. Palau’s newly elected president, Surangel Whipps Jr., called out China’s bullying of his island nation in January 2021, a month after Palauan maritime authorities assisted by the U.S. Coast Guard seized a Chinese vessel suspected of illegally harvesting sea cucumber in Palau’s waters. The PRC’s massive distant-water fleet is considered the world’s biggest perpetrator of illegal, unregulated and unreported (IUU) fishing, which accounts for roughly 30% of all ocean fishing. “With regard to natural resources, China has been aggressively taking advantage of fishing resources in the region,” Satohiro Akimoto, president of the nonprofit Sasakawa Peace Foundation USA, wrote in *The Japan Times* newspaper. “As China has depleted resources in the waters near the coast to feed increasingly demanding consumers at home, the Pacific island region presents opportunities in its vast, rich waters.”

Beijing also wields economic coercion, including retaliating against Palau for its diplomatic ties with Taiwan by essentially banning visits by Chinese tourists, thereby damming a crucial revenue stream for the popular tourist destination. The “challenges confronting the smallest Pacific islands should be front of mind,” Gray, a former Oceania and Indo-Pacific security director at the U.S. National Security Council, wrote in *The Diplomat* magazine in May 2021. “Not only do these states have some of the region’s most strategic

**From left, U.S. Army Maj. Pablo Valerin, Office of Defense Cooperation liaison; Brig. Gen. Falur Rate Laek, vice chief of staff of the Timor-Leste Defense Force; Col. Calisto Santos Coliati, chief of staff of the Timor-Leste Defense Force; U.S. Army Maj. Ruby Gee, Operations in Pacific Island Countries’ Team Timor-Leste officer in charge; and U.S. Army Cpl. Lydia McKinney, Team Timor-Leste cultural liaison noncommissioned officer, tour eastern Timor-Leste.**

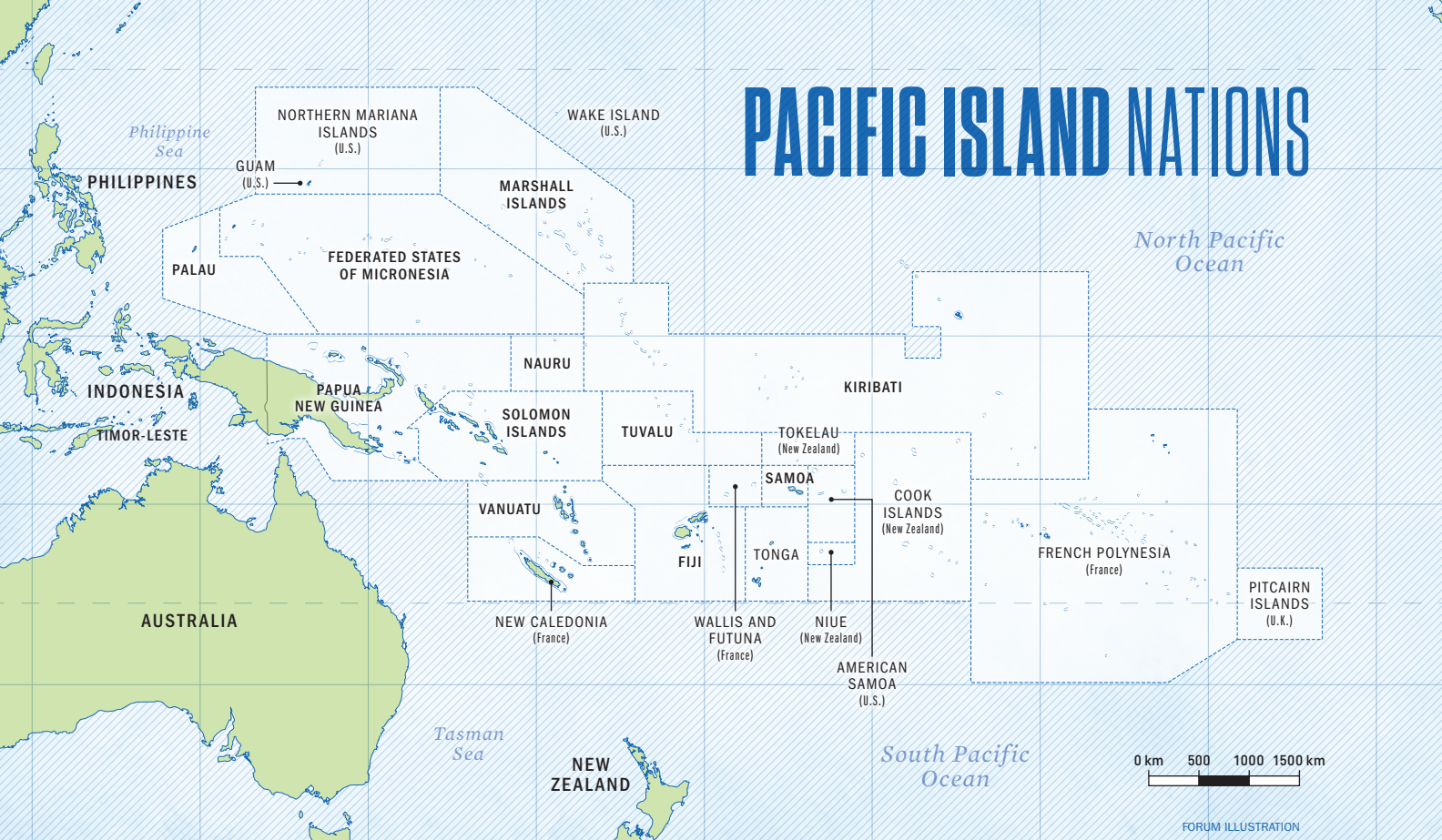
STAFF SGT. SOLOMON NAVARRO/OPERATIONS IN PACIFIC ISLAND COUNTRIES

geography, but they are also committed democracies who have long sought to align with U.S. interests in international forums and at the United Nations.”

### ‘ARENAS OF COMMON PURPOSE’

Collaborative efforts to address those challenges are gathering pace as democratic allies and partners increase their engagement in the region, at least in part, to counter the Chinese Communist Party’s hegemonic ambitions. “One of the things that we are looking to do over the course of the next little while, working closely with allies like Australia, New Zealand, Japan and others, is to convene with Pacific island nations to talk about arenas of common purpose,” Kurt Campbell, the U.S. National Security Council’s Indo-Pacific affairs coordinator, said during a June 2021 event hosted by the Center for a New American Security think tank. “These are islands which we have enormous historical moral and strategic interests in,” Campbell said, according to Reuters. “And, increasingly, again this is an arena of competition both in terms of values, their role at the United Nations, their





health challenges, climate change, their potential role militarily, healthy fishing stocks, just down the list.”

Japan and the U.S. are dialogue partners of PIF (Australia and New Zealand are members) and contribute significantly to the forum. Tokyo has provided U.S. \$580 million in development assistance to the region since 2018, while Washington contributes U.S. \$350 million annually, according to the respective governments. Additionally, the U.S. Agency for International Development’s Climate Ready project has earmarked U.S. \$24 million between 2017 and 2022 to help Pacific island nations and territories mitigate the impact of climate change.

The U.S. also has bilateral shiprider agreements that allow local law enforcement authorities to fight crime within their nation’s EEZ while aboard U.S. Coast Guard vessels. In 2020, the U.S. Army created Operations in Pacific Island Countries to increase its regional presence and assist island nations and territories with the design and implementation of civic aid projects, military and security operations and exercises, and humanitarian assistance and disaster relief programs.

Also in 2020, the U.S. Pacific Fleet hosted the 27th iteration of Rim of the Pacific (RIMPAC), a biennial exercise designed to enhance interoperability and strategic maritime partnerships, which are critical to ensuring the security of sea lanes in support of a Free and Open Indo-Pacific. Conducted at sea around the Hawaiian Islands over two weeks in August, RIMPAC 2020 included 22 ships, 1 submarine and more than 5,300 personnel from 10 partner nations.

In addition to providing financial support in sectors such as education, health and infrastructure, Japan jointly runs the Tokyo-based Pacific Islands Centre, founded in 1996 to assist PIF members with sustainable economic development through the promotion of investment, trade and tourism, according to Japan’s Ministry of Foreign Affairs. Japan also is boosting defense cooperation and exchanges with Pacific island nations as part of its vision for a Free and Open Indo-Pacific, according to its Ministry of Defense. That includes organizing the Japan-Pacific Islands Defense Dialogue — the first-such multilateral defense minister-level meeting — and promoting aircraft visits and port calls by Japan Self-Defense Forces units. “Japan has a unique role to play here as a key ally of the U.S. and as an Asian nation with a long, continuing involvement in the Pacific island nations,” Akimoto wrote in *The Japan Times* in December 2019. “Japan can also emphasize the benefits of economic development and environment sustenance through the values it espouses: rule of law, quality infrastructure and human security.”

## A REGIONAL RESET

Unveiled during a PIF leaders meeting in 2016, Australia’s Pacific Step-up strategy is among the nation’s “highest foreign policy priorities,” with more than U.S. \$1 billion committed to the region in 2020-21 alone, according to Australia’s Department of Foreign Affairs and Trade. During the COVID-19 pandemic, which devastated the region’s vital tourism and service-based





industries, that support expanded to critical supplies. “Australia is the single largest development partner for these nations,” Australian Prime Minister Scott Morrison told the U.N. General Assembly in September 2020. “So, we’ve provided personal protective equipment, testing equipment, medical expertise, and we’re maintaining an essential services and humanitarian corridor so experts and supplies can get in and out.”

Australia’s Pacific Patrol Boat Replacement project, meanwhile, is acquiring 21 vessels through 2023 to replace patrol boats the country donated to 12 Pacific island nations and Timor-Leste between 1987 and 1997, according to the federal government. Part of Australia’s Pacific Maritime Security program, the U.S. \$250 million replacement project will boost the island nations’ ability to patrol their borders, counter IUU fishing and other maritime crime, and conduct search and rescue operations. The 11th of the replacement Guardian-class patrol boats, the RKS Teanoai II, was presented to Kiribati in June 2021.

Like its neighbor across the Tasman Sea, New Zealand has stepped up its regional engagement. In a February 2019 statement, Morrison and New Zealand Prime Minister Jacinda Ardern noted that “the prosperity and security of the Pacific was of fundamental importance” to their nations, agreeing to amplify their partnerships with island nations and territories. Under its Pacific Reset policy launched in 2018, New Zealand has augmented its aid funding, increased the frequency of ministerial-level meetings and created more than a

dozen new diplomatic and development posts focused on the region. In mid-2020, it established a resident defense advisor in Tonga to coordinate operations such as disaster response. The NZDF is providing professional leadership training to island nations “to embed the fundamentals of ethical and effective leadership among Pacific security personnel,” while also enhancing and realigning its resources to support amphibious operations and maritime patrols in the Pacific region. “An array of challenges facing the Pacific, from climate change to geostrategic competition, requires more from us and our like-minded partners,” the NZDF’s “Advancing Pacific Partnerships” report noted.

Indeed, as they face threats both immediate and existential, Pacific island nations will lean on Australia, Japan, New Zealand and the U.S., as well as friends elsewhere in the Indo-Pacific, Europe and around the globe. “As a small nation, we can easily be infiltrated, and we depend on our partners to protect us and give us security,” Whipples, the Palauan president, said during a March 2021 trip to Taiwan. As if to heighten Whipples’ concerns about the fragility of sovereignty, China’s People’s Liberation Army sent 10 military aircraft into Taiwan’s air defense identification zone while he visited the self-governed island claimed by Beijing.

“With Beijing’s ambitions growing rapidly,” Gray, of the American Foreign Policy Council, wrote in *The Diplomat*, “it will require a combined effort by Washington and its allies to ensure the Indo-Pacific’s smallest states continue to enjoy independence, security and prosperity.” □





# BLACK MARKET FOREIGN EXCHANGE

FORUM ILLUSTRATION



# *Chinese Communist Party members move money in plain sight, threatening security*

JOHN F. TOBON/U.S. HOMELAND SECURITY INVESTIGATIONS

**A**uthorities uncovered a scheme in 2020 in which Chinese money brokers were reportedly colluding with Mexican drug traffickers to launder money. Officials interpreted the unlikely pairing as the latest example of trade being used to conceal illicit funds. Investigators, however, were only seeing one side of a very complex set of transactions mainly designed to evade foreign exchange restrictions, not launder illicit funds.

Foreign exchange (FOREX) is critical to global economic stability. It is the centerpiece of licit and illicit world trade, facilitating the movement of goods and services. It is also a lucrative business: Fortunes are won and lost as the result of fluctuations in the currency markets, and entire economies hinge on it.

The scheme uncovered by the authorities involved black-market FOREX (BMFX). The significance of BMFX to illegal actors has been, at best, grossly underestimated and, at worst, completely overlooked. For many years, the relationship involving international trade, BMFX and illicit actors has been correctly seen as a money laundering vulnerability. However, the key factor in this equation has been erroneously interpreted to be the trade, hence the moniker trade-based money laundering.

A closer examination of the relationship among these factors, along with historical analysis and future forecasting, reveals that first, the key to unraveling these laundering schemes is the BMFX and not the trade; and second, that when the People's Republic of China (PRC) is involved, BMFX can have national security implications for the United States and other nations.

This article examines the importance of BMFX to licit and illicit enterprises. It explores the impact that BMFX has on the Indo-Pacific region and analyzes the impact that FOREX restrictions in China had on BMFX markets in Latin America. Lastly, it charts the informal partnership of convenience among Chinese BMFX brokers, Latin American criminal organizations and Chinese politically exposed persons (PEPs) (those entrusted with a prominent public function).

## **CURRENCY RESTRICTIONS AS A CATALYST FOR ILLICIT ACTIVITY**

Parallel currency markets are a fixture of countries around the world. The economic policies that give



**Chinese and U.S. bank notes** REUTERS

rise to BMFX are often undertaken to avoid national economic catastrophes. They frequently are precipitated by devaluation of the national currency, resulting in increased demand for foreign currency, usually U.S. dollars (USDs). The increased demand has the practical effect of pushing the value of the national currency further down.

To counter the impact of these actions on the economy, nations restrict the purchase of FOREX, the outbound movement of physical currency, as well as control the repatriation of FOREX held overseas by its exporters. Such policies make it difficult, or even impossible, for importers to purchase the FOREX they need to run their business.

At the same time, the restrictions have the effect of disincentivizing exporters who earn FOREX for their goods. The price of the FOREX will be too high for importers to purchase and too low for exporters to sell. The policies create a heavy burden for those in the economy who rely on FOREX as part of their business model, while they create opportunities for those who have access to or possess FOREX outside the regulated market.

Black markets for USDs in the Indo-Pacific have existed for decades. These markets, some dating to the 1940s, began as a result of FOREX controls put in place by various nations, according to analysts. These controls effectively cut off access to USDs for individuals who use the currency to participate in international trade.



This situation generated demand for USDs outside the regulated FOREX sector, creating the black market. FOREX markets, whether formal or informal, operate by supply and demand. When a black market is born, the demand for an alternative source of USDs will be met through illicitly sourced FOREX, often in the form of high-level political corruption, and criminal activity — primarily, drug trafficking.

## FOREX MONEY LAUNDERING

The laundering process in this scenario continues to confuse and perplex government entities and the business community. How do business transactions become tainted with the proceeds of criminal activity? How does that taint give rise to the necessity for businesses to commit further crimes to conceal their collaboration with criminal organizations? The million-dollar question: When does the laundering occur?

Business transactions become entangled with criminal activity when importers purchase FOREX from BMFX brokers. These brokers are the link between the illicit supply of FOREX and the pseudo-legitimate demand. The legitimacy of the demand is called into question because illicit FOREX is used to purchase legitimate products as part of a traditional international trade transaction. The importer must now find a way to complete the importation.

organizations, such as the Financial Action Task Force, have advocated for more scrutiny of international trade transactions to identify and curb money laundering. Unfortunately, the laundering that everyone is so concerned with occurred before the goods were even purchased. The criminal organization that earned the illicit FOREX removed itself from the picture when it sold its FOREX to the BMFX broker. Criminal organizations consign products to their customers, but they won't consign their proceeds to money brokers. The trade-based money laundering model erroneously assumes that criminal organizations will invest their proceeds in legitimate goods so they can collect their laundered proceeds once the goods are imported and sold.

This line of thinking has a critical flaw. It assumes that the criminal organization is in cahoots with the importer. As a result, some believe that following the trade will lead to the source of the illicit FOREX. That mindset has diverted attention and resources away from the true vulnerability, as well as overlooked criminal and fiscal violations committed by the importer.

Instead of tasking financial institutions with looking at trade transactions — for which they are ill-suited — resources should be marshaled to review the accounts that supply the funds to purchase the goods. This will identify the supply side of the BMFX, the criminal organizations and corrupt politicians.

## OVERLAP OF CHINESE BLACK MARKET AND MEXICAN TRAFFICKERS

Nowhere is this confusion more evident than in the relationship between the BMFX in China and Mexican drug trafficking organizations (DTOs). This stems from a myopic interpretation of events, combined with an uninformed view of BMFX. News headlines state that Chinese money launderers are at the service of Mexican DTOs, which assumes that the brokers are working primarily for the criminals' benefit.

But are they? The answer requires a wider view of BMFX in China, where it has thrived for many decades. The Chinese BMFX has been supplied by smuggling, overinvoicing of imports, underinvoicing of exports, remittances received from abroad and border trading, analysts explain. The supply of FOREX to the Chinese BMFX had been sufficient to meet the demand. This changed with the implementation of China's FOREX rules in July 2017, which require banks and financial institutions to report domestic and overseas cash transactions of 50,000 yuan (U.S. \$7,820) or more. Banks are also required to report overseas transfers of U.S. \$10,000 or more. Additionally, the rules created a U.S. \$50,000 foreign exchange limit.

This policy change sought to curb corruption by Chinese Communist Party (CCP) members and officers of state-owned enterprises. Specifically, it was aimed at restricting the ability of Chinese nationals to buy overseas property, securities, life insurance or other



An electronic board shows foreign exchange rates in Hong Kong.

AFP/GETTY IMAGES

The methods used to complete the importation necessitate the use of customs fraud schemes (over/under valuation or double invoicing), smuggling and/or bribery of public officials. This is also how government entities and financial institutions begin their trip down the trade rabbit hole. This combination of factors is what is usually described as trade-based money laundering.

Highlighting the importance of the trade transaction makes it seem as if trade is the key node in this scheme. Law enforcement and international standard-setting



Men sit outside the Bank of China headquarters in Beijing.

THE ASSOCIATED PRESS

investment-style insurance products. Prior to this policy revision, CCP members were able to use traditional FOREX markets and conventional banking practices to move and enjoy their wealth overseas. These restrictions did not curb corruption. They did, however, have the unintended consequence of pushing demand for USDs on the Chinese BMFX beyond existing supply. Because the BMFX works like traditional FOREX markets, Chinese BMFX brokers were forced to seek new sources of USDs to meet demand. This is how Mexican DTOs entered the equation. Chinese money brokers sought USDs held by Mexican DTOs as a means to supply their ultimate customers, Chinese PEPs who need USDs to secure their financial future outside China. The laundering that occurs for the Mexican DTOs is an ancillary activity, merely a means to an end for Chinese money brokers.

### CHINA AND REAL ESTATE

The manifestation of this can be seen throughout North America, the Indo-Pacific and Oceania. Over the past decade, cash purchases of luxury real estate by Chinese PEPs have been increasing in Australia, Canada, Hawaii and points in between. Chinese money brokers can leverage arbitrage between the two forms of yuan — the onshore renminbi and the offshore renminbi — to move value from mainland China to Hong Kong. Once the value is in Hong Kong, they can take advantage of the free-market environment that is outside the influence of the People's Bank of China.

Chinese money brokers then use USD accounts held in the name of shell corporations within Hong Kong

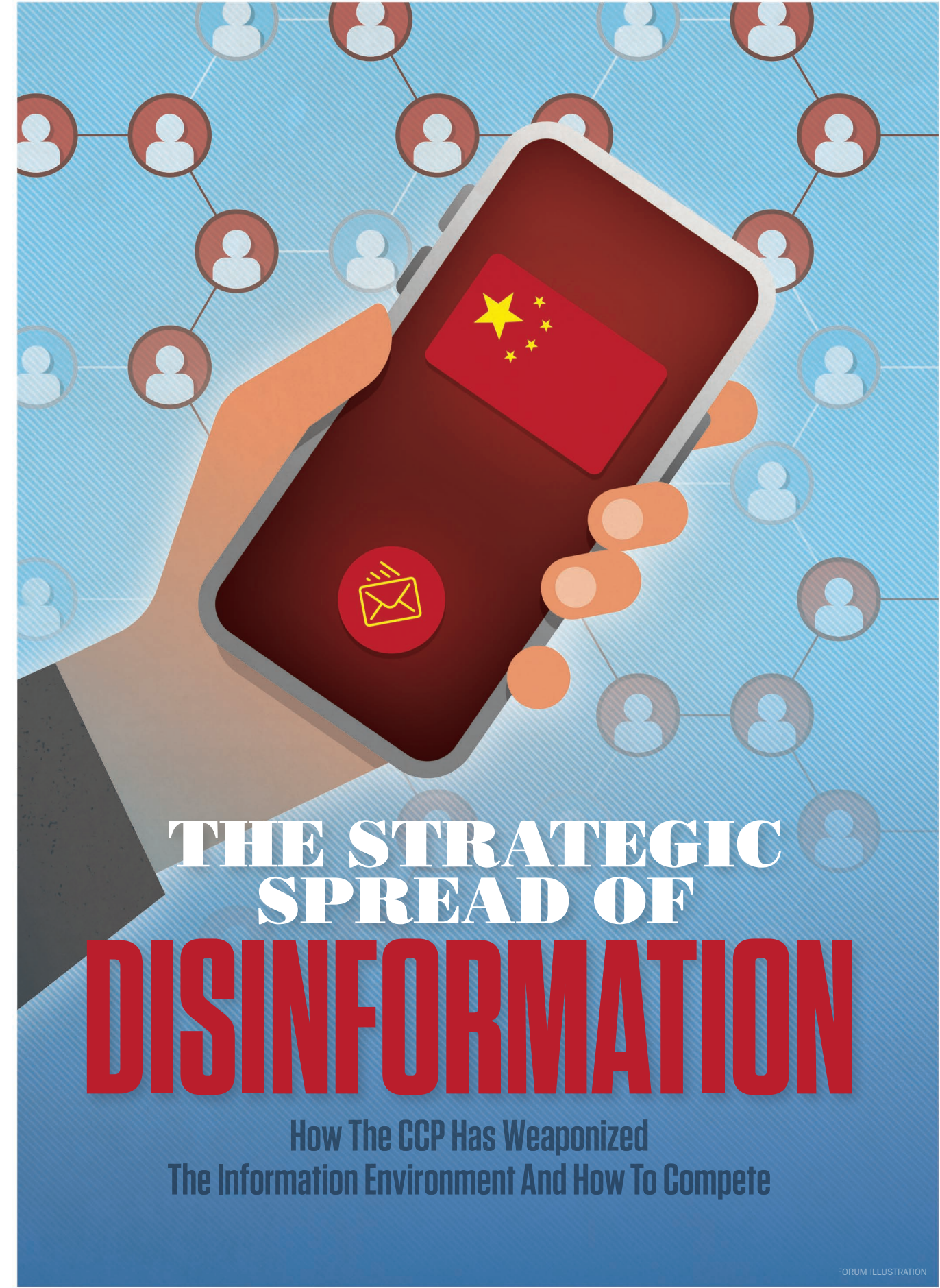
financial institutions to send third-party wire transfers worldwide. These USDs, purchased by Chinese BMFX brokers from sources including Mexican DTOs, are then sold to Chinese PEPs. When the wires arrive in U.S. financial institutions, the recipients often cite China's currency restrictions as the reason why the transactions look odd.

Until recently, financial institutions were sympathetic to their customers and did not question the transactions. As they have been provided with a broader picture of the scheme, they have started to scrutinize such transactions.

### STOPPING ILLICIT TRANSFERS

The national security implications of money laundering via FOREX involving Chinese PEPs are significant. If law enforcement continues to focus on the supply side of the Chinese BMFX, authorities will disrupt efforts to procure USDs from Mexican DTOs. However, the sources of illicit FOREX are too numerous to count. Investigative efforts must factor the complex nature of the threat. These schemes must no longer be seen as circular transactions involving two parties with common interests. Instead, they must be seen for what they are — arm's-length transactions that are part of a larger underground industry essential to the operations of disparate criminal groups worldwide. Failure to do so will allow Chinese PEPs to continue to move their illicit gains to Western cities, where those funds will be available for legitimate activities such as gambling and high-end real estate purchases, as well as for sinister activities that can include meddling in domestic politics. □





# THE STRATEGIC SPREAD OF DISINFORMATION

How The CCP Has Weaponized  
The Information Environment And How To Compete

FORUM ILLUSTRATION

Soon after Chinese Communist Party (CCP) General Secretary Xi Jinping came to power, the CCP's Central Committee General Office circulated a communique that came to be known as Document 9. It unequivocally stressed unwavering adherence to the party's control of media and concerted management of the ideological battlefield, which analysts interpreted as a drastic departure from the party's previous emphasis on domestic political control and censorship. Under Xi, the CCP has greatly expanded its influence operations in the information environment to manipulate the rest of the world. One of the key party organizations tasked with this mandate is the United Front Work Department (UFWD).

Spearheaded by the UFWD, the CCP has used disinformation campaigns on social media and news media platforms and artificial intelligence-enabled censorship of any voice that contests CCP propaganda. Its messaging has had several key themes. For instance, the CCP has consistently attempted to convince foreign audiences that it is a responsible and benevolent world leader by presenting the CCP's autocratic model as a credible alternative to the West. Similarly, the CCP has attempted to undermine the perceived legitimacy of elections and democracy. It has consistently used disinformation campaigns to disrupt political processes in democratic countries.

These incidents indicate an increasing sophistication of the CCP's information operations. As a whole, they pose far greater threats to the national security of the United States and other democratic nations than before. The U.S. and its allies and partner nations should approach the information environment as one of the most critical arenas of great power competition between democracies and autocracies. This article highlights the key characteristics of CCP information operations observed since 2020. Then, it offers three recommendations on how to combat this increasingly disruptive and distributed threat.

The year 2020 proved a watershed moment for those who have analyzed the CCP's disinformation efforts. Its campaign to distort the truth about the COVID-19 virus showed an incredible reach with brazen official statements. The CCP sought to convince domestic and global audiences that the virus was intentionally planted in Wuhan, China, as a U.S. bioweapon. The campaign's reach was vast, with propagation by the Chinese Foreign Ministry and its diplomats, government leadership and foreign policy figureheads in Iran, Russia, Saudi Arabia and Venezuela, among others, and an array of online media sources. It also showed an expanded network of



**Investigators discovered a vast social media campaign by the Chinese Communist Party in 2020 to mischaracterize the United States' activities in the South China Sea. The campaign on Facebook and other platforms gained over 130,000 followers and sought to realign the Philippines with China.**

transnational collusion. For example, Global Research Canada, a Canadian conspiracy website, and CCP officials often cited each other for validation. This disinformation tactic, known as "information laundering," involves propagation of disinformation by purported Western analysts and media as a means of legitimizing the CCP's disinformation campaign. Similarly, Chinese Foreign Ministry spokesman Zhao Lijian's false tweet about COVID-19's origin in March 2020 was retweeted over 99,000 times, in at least 54 languages, and reached roughly 275 million people collectively.

## INDO-PACIFIC BATTLEGROUND

While the CCP's information warfare has become truly global, the Indo-Pacific region has received the brunt of Beijing's disinformation campaigns. In particular, the CCP's efforts to mischaracterize Hong Kong's 2019 pro-democracy movement showed sophisticated information operations. The CCP used its broad media infrastructure to propagate false claims of pro-democracy activists' collusion with foreign actors. In a similar vein, the CCP has targeted Taiwan to undermine its political independence and social cohesion. For instance, the CCP's attempt to prop up pro-Beijing Kuomintang mayoral candidate Han Kuo-Yu in a ruling Democratic Progressive Party (DPP) stronghold in 2018 was highly impactful. False narratives and doctored images originating from the People's Republic of China (PRC) and its affiliates spread widely on social media, vilifying the DPP government and praising Han. The CCP also





**Chinese Foreign Ministry spokesman Zhao Lijian's false tweet about the origins of the COVID-19 virus in March 2020 was retweeted over 99,000 times, in at least 54 languages, and reached roughly 275 million people collectively.**

attempted to sway the 2020 Taiwan presidential election, but Taiwan was prepared. Greater media literacy and disinformation mitigation enabled by public and private partnerships played a critical role.

The CCP's information operations designed to undermine the region's stability and erode the U.S.'s strategic interests were not limited to Taiwan and Hong Kong. Responding to investigative reporting that exposed a massive scale of concentration camps, rampant disappearances, extrajudicial murders and forced sterilization, the CCP went on the offensive to distort the truth. The CCP has globally disseminated false claims of economic development and education in China's Xinjiang region to mask its ongoing genocidal campaign against ethnic Uyghurs and other minorities. The CCP has also restricted foreign journalists from entering the region to monopolize information emanating from Xinjiang. In Thailand, a fake video campaign allegedly depicting an Asian being brutally assaulted in the U.S. appeared on social media in 2020. The intent was to trigger and spread anti-U.S. sentiment in Thailand. The video was widely shared by pro-Beijing outlets and went viral in Thailand. In reality, the video clip was taken from a prison riot in Ecuador. This was not an isolated incident. The Philippines has also been subjected to a concerted disinformation campaign on social media to mischaracterize U.S. activities in the South China Sea. This campaign amplified statements of local politicians sympathetic to the CCP, gaining over 130,000 followers and seeking to realign the Philippines with China. In short, CCP disinformation efforts in recent years have dramatically grown in scope and intensity. Three patterns characterize competition against the CCP in the information environment. First, the CCP has greatly exploited asymmetrical access to media platforms. While major Western social media platforms such as Facebook and Twitter have few or no access restrictions for authoritarian regimes, Chinese social media counterparts

such as WeChat, Sina Weibo, Tencent Weibo and Tencent QQ have varying levels of access restrictions to Western users. Furthermore, the CCP exploits its social media platforms for censorship and surveillance. Data from foreign usage of these platforms is likely aggregated by the CCP for collection and intelligence purposes. Users in mainland China cannot access most Western news media and social media platforms. This makes it challenging for Western efforts to understand domestic CCP disinformation efforts and to aggregate data on these platforms.

Second, the CCP has dramatically increased its online presence globally since the COVID-19 pandemic hit the world. CCP officials' activities on Western social media platforms have reached a record-setting level. For instance, CCP diplomats tweeted 210,382 times, averaging 778 times a day, over nine months in 2020.

Third, CCP intelligence services rely heavily on state-controlled technology companies to weaponize massive amounts of data for surveillance and censorship. This practice is not something the U.S. and its allies could simply emulate without severely encroaching on democratic principles and norms. CCP-affiliated companies are known to install backdoors to their technology that can enable offensive cyber operations. Similarly, the CCP has dramatically increased its cyber-enabled espionage and hacking in the region.

In sum, information warfare is one of the most critical arenas of great power competition. Moreover, the extent to which the CCP has weaponized the information environment poses grave national security threats to the region and beyond. The U.S. and its allies and partner nations should integrate data-driven open source intelligence in routine military planning and operations. The following strategies can combat the rapid expansion of CCP propaganda.

## COMPETING IN THE INFORMATION ENVIRONMENT

First, the so-called whack-a-troll approach will not be sufficient to combat CCP disinformation because malign actors can either migrate to other platforms or change their user accounts. The CCP can always manufacture or contract out more accounts faster than other governments or companies can remove them from the information environment. Rather, governments should treat disinformation as a full-spectrum continuous campaign. More specifically, those who are responsible for safeguarding the integrity of the information environment should consider the following:

- Continuously observe disinformation sources, dissemination mechanisms and effects. Much like operating in the land domain, it is critical to map and share how adversaries command, control, maneuver and communicate in the informational battleground.



**Taiwan President Tsai Ing-wen celebrates her January 2020 reelection with supporters in Taipei. The Chinese Communist Party attempted to influence the election in favor of Tsai's opponent, but failed due to greater media literacy and disinformation mitigation enabled by public and private partnerships.**

- Orient toward the entire system of disinformation propagation. Disinformation, much like any other weapons system, has an identifiable supply chain. While it is nearly impossible to attack domains in the PRC, CCP disinformation heavily relies on regional and local media outlets.
- Decide on appropriate courses of proactive action from a whole-of-society perspective. It is critical to note that governments alone are often insufficient to combat the impact of malign content because much of the threat exists in commercial or civilian networks. Working with industry and civil society is a key decision to consider.
- Act on the best available solutions to actualize the most appropriate course of action. A good example of this step is Taiwan's Digital Accountability Project to promote fact checking and exposing compromised media outlets.

Second, government and industry leaders should expect foreign and extremist information operations to be more intense and rampant during any crisis. COVID-19 was an example of how authoritarian regimes exploit disinformation to exacerbate crises in democracies. Put differently, it is paramount that the public and private sectors develop resident systems to guard their assets and constituents against malicious information operations

especially during an emerging crisis. Such endeavors should also include proactive messaging to inoculate their respective audiences from externally motivated and disruptive information operations.

Third, government and industry leaders should further embrace and promote public and private partnerships (PPPs) to accelerate the integration of mature technological solutions. For instance, the U.S. government should help its allies and partner nations to replicate and coordinate innovation partnership programs, such as the Defense Innovation Unit and the National Security Innovation Network under the U.S. Defense Department's Defense Innovation Board. In essence, democratic countries will be able to collaborate to scale and distribute how to compete against the CCP's information warfare as an alliance of open societies.

A whole-of-society approach is not an option but rather a prerequisite to compete effectively against the CCP in the information environment. This approach would involve a more persistent PPP framework in which each government agency responsible for information statecraft has an advisory council of think tanks, academics and private sector stakeholders. This council of experts would convene regularly to discuss strategic challenges to open society and economics and to seek solutions unhindered by confirmation bias or bureaucracy. □





# ECONOMIC CONFLICT WITH **CHINA**

# Meeting the Threat Together

DR. SHALE HOROWITZ/UNIVERSITY OF WISCONSIN-MILWAUKEE

China's economic rise no longer looks like a benign story of inward-looking development and international coexistence. Under General Secretary Xi Jinping in particular, the characteristic Chinese Communist Party (CCP) methods of internal economic and political control have become more centralizing and repressive. Foreign policies are more overtly aggressive. These policy changes have come as China's economy moves into a more capital-intensive specialization. This presents other nations — particularly in the Indo-Pacific region — with a raft of major new economic security threats, which often compound worsening military security threats.

How can threatened states best respond? To answer this complex question, it helps to categorize the variety of threats and response capacities. Powerful countries that face economic and military threats from the CCP are likely to form the strongest coalition advancing the most effective responses. These states, in turn, are likely to attract the cooperation of a second important group of states, which face threats that are primarily economic. This is illustrated by examining three threats to infrastructure and supply chain security — in telecommunications, rare earth minerals and semiconductors — and an example of interstate policy coordination — the Supply Chain Resilience Initiative (SCRI) of Australia, India and Japan.

This theory and evidence support the conclusion that China's threats are calling forth an alternative core group of states. This core has the will and ability to prevent China from using economic leverage to force unwilling states into economic dependence that also may threaten their diplomatic autonomy and military security. The case studies also suggest guidelines for building best responses to China's threats. These include starting at home with state-level policies; cooperating as closely as possible with like-minded alternative core states; supplementing these foundational policies with efforts to advance and popularize compatible international norms; and avoiding policy errors by focusing on specific threats and working with allies and partners to face them directly and efficiently.

## **The China Economic Threat: Goals and Strategies**

During the Xi period, China's economic ambitions have changed qualitatively. China no longer seeks

to integrate into the international economy merely as part of the “reform and opening up” campaign to modernize its economy. This modernization has now reached a transitional phase, where China has mastered labor-intensive production and is moving into more capital-intensive sectors that compete directly with the world's advanced economies. Xi aims to vault China into a dominant position across all major high-technology industries, rather than merely allow market forces to direct China into the one-among-many type of division of labor now prevailing among advanced economies.

How is this goal to be achieved? Formally, as with the Made in China 2025 plan and its iterations, the main instruments are to be state subsidies and, in select strategic sectors such as telecommunications, a guaranteed home market. Informally, there are additional powerful instruments. One is a broader discrimination against foreign-owned firms competing in the home market, designed to force transfer of their technology to local partners and then use regulatory discrimination and subsidies to replace them entirely with domestic producers. Simultaneously, an unprecedented campaign of state-sponsored cyber theft is being used to steal foreign technology directly. China's domestic producers ultimately shift focus to export markets, again supported by direct subsidies and a protected home market. States that openly criticize these efforts or take countermeasures are threatened with accelerated targeting of their remaining markets in China and reduced visits by Chinese tourists and students. The same treatment is meted out to states that disagree with China's other foreign and domestic policies.

As consolidation of high-tech industries in China takes hold, other nations' economies will become more dependent and vulnerable. Their economies will be in a subordinate, replaceable position in supply chains, with China having asymmetric leverage. For countries involved in territorial disputes with Beijing, there are even darker prospects. Such threats are credible because of China's size; and because China can usually compartmentalize such conflicts to the major vulnerabilities of targeted states as these and other states are typically not willing to respond in kind or escalate.



CHINESE THREAT LEVELS AND TARGET RESPONSE CAPABILITIES			
	Militarily and Economically Threatened	Economically Threatened; Military Threat Limited or Absent	Less Significantly Threatened
More Powerful	The Quad (Australia, India, Japan, United States), Taiwan, Vietnam	Canada, European Union, Indonesia, South Korea, United Kingdom	Bangladesh, Ethiopia and others
Less Powerful	Philippines; smaller Pacific island states	Malaysia, New Zealand, Singapore, Thailand	Most lower-income developing countries

NOTE: More powerful states have greater comprehensive capabilities, involving population, per capita income and state capacity. Threats are significant both militarily and economically, only economically or in neither area.

Table 1

**“As consolidation of high-tech industries in China takes hold, other nations’ economies will become more dependent and vulnerable.”**

#### Types of Chinese Threats and Target Response Capabilities

Although China’s economic threat has a uniform logic, countries face different threats and possess different response capabilities (Table 1). States facing military as well as economic threats from China have the strongest motivation to respond comprehensively. For example, the member states of the Quadrilateral Security Dialogue (Quad) — Australia, India, Japan and the United States — fit this category. For countries that are only or primarily threatened economically, the threat varies with the level of development. Developed nations face threats to their existing specializations in more capital-intensive goods and services, while middle-income states face threats to their ability to continue moving up the value chain into more capital-intensive specializations. Lower-income countries are least threatened since movement upward into capital-intensive specializations is a longer-term prospect. Such lower-income countries are faced mainly with exclusion from China’s lucrative domestic market if they do not follow Beijing’s lead or at least remain neutral in foreign policy matters.

Nations also have different response capacities, and efforts to craft joint responses to counter China’s threats must account for such differences. Trying to impose excessively uniform responses will produce lowest-common-denominator policies, and even these are unlikely to be reliably implemented. By evaluating responses already taken to meet specific threats to specific states, the type of flexible, cumulative policies likely to be most effective will become apparent.

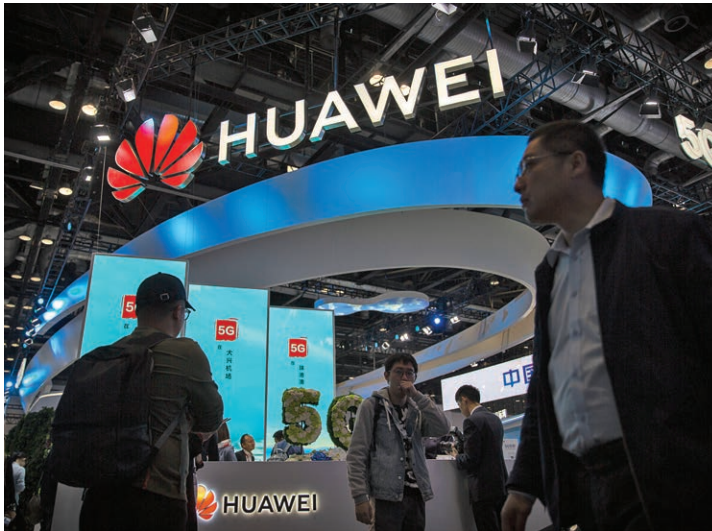
#### Threat Responses Take Shape:

##### Critical Infrastructure and Supply Chains

Responses to China’s economic threats have been most far-reaching where Chinese suppliers have developed the capacity to control or disrupt vital infrastructure and supply chains. The most prominent example of critical infrastructure has been telecommunications network equipment, where Chinese companies led by Huawei have established a dominant global market position on the basis of leading-edge products sold at prices significantly lower than those of the competition — mainly the European companies Ericsson and Nokia and the South Korean company Samsung. Huawei’s dominance has been built largely on technology theft, subsidies and a privileged home market position. But Huawei would pose serious threats even had its position been won fairly. Access to foreign networks would enable the CCP regime to inject malicious software and spy on communications, and to orchestrate large-scale, potentially long-lasting disruptions or outages in network-dependent infrastructure and services.

Such threats loomed large as Huawei looked set to become the major supplier of new 5G networks. The response has been surprisingly effective. Bipartisan consensus in the U.S. Congress led to an early ban on equipment from Huawei, ZTE and other Chinese suppliers in U.S. networks. The U.S. administration under then-President Donald Trump explained the risks publicly, adding that intelligence cooperation with allies would be compromised by Huawei equipment. In addition to advocating outright bans, the Trump administration supported a Clean Network initiative, which, without explicitly mentioning China, sought coordination by governments, organizations and businesses to maintain reliable and secure networks — and related businesses, such as applications, cloud services, and computer and other hardware. The initiative builds on similar, complementary efforts, such as the European Union’s 5G Clean Toolbox.

Governments, fearing CCP economic retaliation, were often publicly resistant to formal bans on Chinese



Huawei's 5G services are displayed at a Beijing expo. THE ASSOCIATED PRESS

5G equipment. Yet many already harbored doubts, and the resulting debate raised popular awareness about the risks. The result was a broad array of formal and informal bans on Huawei and other Chinese equipment. The Clean Network initiative is now supported by over 60 countries, including almost all members of NATO, the EU and the Organisation for Economic Co-operation and Development, together accounting for over two-thirds of global gross domestic product, and by hundreds of important private companies providing telecommunications services and related software and hardware.

The pattern of national responses is broadly consistent with the varied pattern of military and economic threats. All states facing significant military threats from China adopted formal or informal bans, as did most states facing significant economic threats. Far fewer states did so where neither type of threat is notable. Nevertheless, significant progress is possible even in the little-or-no-threat category. Here, President Trump's administration also facilitated decisions of favorably disposed states by setting up the International Development Finance Corp. (DFC) and expanding the authority of the U.S. Export-Import Bank to offset China's subsidized financing and thus make bids from alternative suppliers more competitive. DFC financing facilitated Ethiopia's recent choice to use a European-led, "clean" consortium to build its 5G network.

Rare earth minerals are necessary for industrial processes in important sectors such as electronics, renewable energy and military hardware. Beginning in the 1990s, China assumed a dominant position in production and processing of rare earths. In 2010, China intensified export restrictions, both to punish Japan over an island dispute in the East China Sea and to provide cost advantages to domestic users. China's exports ramped up again from 2015, but the episode showed the dangers of economic dependence on China.

Japan, given the importance of rare earths to its industries, reacted quickly. Japan's government invested in rare earth mines outside China, reducing its dependence on Chinese supplies from above 90% in 2010 to under 60% in 2020. The

## Three Principles for Optimizing Threat Responses of Allies and Partners

**Principle 1: Building and guarding a country's own strength is the only realistic and reliable foundation for security.**

Each state threatened by China must respond with its own strategy, tailored to its own threats and capacities. States more threatened by China will feel the need to take more far-reaching countermeasures. Those states with limited means will try to avoid becoming the focus of Chinese Communist Party ire and sanctions by speaking softly and acting more informally. Nevertheless, such states are not the same as largely unthreatened, indifferent neutrals and should be assisted by allies and partners in the same soft-spoken and informal manner.

**Principle 2: Work together flexibly to maximize security within or alongside an alternative core group of states.**

The most threatened and capable states, flexibly acting together in pursuit of the common goals of military and economic security, form a natural alternative core in the world economy with the capacity to better protect their joint security and independence, while offering similar benefits to less threatened states. Because of the varied situations of these states, and the fast-changing security issues raised by various sectors and supply chains, different approaches to economic and military security will be necessary. Such a patchwork is complex and hard to manage but necessary.

**Principle 3: Calibrate responses to threats, while preserving sound principles of national security and economic development.**

The most critical infrastructure and supply chains to be secured in the alternative core will naturally tend to mirror those that the CCP regime most jealously reserves for its own control. The CCP regime, by its increasingly brazen intrusiveness, propels the process of defensive reaction. The dual-use manner in which measures taken by Chinese firms to protect the CCP's internal political control and national security are seamlessly used abroad to control and threaten other states almost necessitates excluding or limiting the presence of such firms in any state that feels threatened.

Threatened states should focus on effectively working together to minimize such Chinese threats, without departing from traditional sound principles of national security and economic development. States must protect critical infrastructure and supply chains, using an inner circle of more secure supply for emergency use in wartime, along with an outer circle where a broader, freer division of labor develops among mutually trustworthy partners.





Lynas Corp.'s rare earth minerals processing plant in Gebeng, Malaysia, is pictured while under construction in 2012. After China imposed export restrictions, Japan's government invested in rare earth mines outside China, reducing its dependence on Chinese supplies from above 90% in 2010 to under 60% in 2020.

THE ASSOCIATED PRESS

Technical and market demand considerations should determine the minimum secure scale of such mining and processing facilities, such that production and stockpiles are sufficient to guard against potential disruptions from China under peacetime conditions and plausible conflict scenarios.



U.S. built on Japan's work with Australia. Relatively small U.S. government subsidies sufficed to encourage not only rare earth mining in the U.S. but also U.S.-based rare earth processing by the Australian company Lynas and other firms.

The U.S. also signed purchasing agreements to encourage rare earth mining in reliable sources such as Australia and Canada. Technical and market demand considerations should determine the minimum secure scale of such mining and processing facilities, such that production and stockpiles are sufficient to guard against potential disruptions from China under peacetime conditions and plausible conflict scenarios. Such capabilities also provide similar levels of security to vulnerable allies and partners, which might otherwise have little alternative to Chinese supplies. Similar beginnings on building reliable local capacities for rare earth mining and processing, underway in some Southeast Asian countries, also merit support from Australia, Japan, the U.S. and other concerned states.

In recent years, semiconductors have presented an even more important supply chain security problem. Semiconductors perform the control, calculating and storage functions at the core of electronic equipment and almost all other machines. As the capital-intensity of semiconductor fabrication plants (fabs) has ballooned along with the state subsidies used to attract them, U.S. and other companies have focused on chip design while outsourcing production. The U.S. share of global production thus fell from 37% in 1990 to around 12% in 2021. Production has increasingly shifted to the Taiwan producer TSMC and the South Korean producers Samsung and SK hynix. TSMC has become the world's largest contract producer of semiconductors and in recent years, as more electronics manufacturing has moved to China, has built more of its fabs in mainland China.

During President Trump's administration, there was significant progress "reshoring" semiconductor manufacturing in the U.S. Significantly, this was achieved primarily via cooperation with the biggest foreign producers — TSMC and Samsung. TSMC is moving ahead with a huge fab complex in Arizona, while Samsung is developing one in Texas. How were these advances possible? First, the various levels of U.S. government finally began offering the large subsidies provided by other states. Second, once the U.S. government decided that a larger domestic semiconductor production base was necessary for economic and military security, both TSMC and Samsung quickly understood that having such a presence in the U.S. was desirable. If they did not capitalize on the opportunity, their competitors would, placing them at risk of losing market share in the U.S. and elsewhere. Moreover, by diversifying supply chains and limiting dependence on production in China, the firms limit China's ability to hold their non-Chinese markets hostage to force greater dependence



**Taiwan's TSMC, the world's largest contract producer of semiconductors, has been building its fabrication plants in China in recent years. REUTERS**

on production in China and technology transfer to Chinese firms. A large U.S. base gives TSMC the option of expanding production beyond the reach of China and hence reduces China's ability to threaten the company. In effect, TSMC has chosen to remain an independent company by securely diversifying its production base beyond Taiwan and China, rather than allowing itself to be slowly transformed into a Chinese-controlled entity by a combination of incentives and threats. To a lesser extent, the same is true for Samsung.

The decisions by these flagship companies similarly advance the economic and national security interests of Taiwan and South Korea. Notably, both Taiwan, due to the intensifying military and economic absorption threats from China, and South Korea, following China's economic sanctions imposed in response to South Korea's missile defense efforts, had already begun diversifying supply chains prior to the worsening of U.S.-China trade relations in 2019. For the U.S., there is a parallel to the vicissitudes of its domestic auto industry in the 1970s and 1980s. Strength is best maintained or rebuilt not by artificially propping up privileged home-market champions but by attracting the most efficient foreign firms to produce locally and thus forcing domestic firms to maintain competitiveness.

### **Working Together for Supply Chain Resilience**

While states' responses to China's threats necessarily reflect their own vulnerabilities and capacities, they are most effective when regularly and flexibly coordinated in the service of common long-term objectives. An important example of such coordination is the SCRI launched in 2021 by Australia, India and Japan. The initiative is intended to promote supply chain security by sharing best practices and by promoting investment and "buyer-seller matching." This coordination is facilitated by the way in which each state's measures to address vulnerabilities inherently tend to complement the others' efforts.





**A worker stacks buckets at an aluminum factory in Agartala, India. In 2020, the Indian government announced broad subsidies for incremental sales increases from domestic production across 10 major industries.** REUTERS

Japan's greatest unnecessary dependence on China is in using Chinese suppliers as crucial parts of supply chains for re-export to Japan and foreign markets. Japanese producers do not want to give up on the Chinese market unless forced to do so. But neither do they want China to be able to hold hostage their ability to supply other markets; nor are they interested in basing their highest-end technology and production in China, where it can be most easily appropriated by Chinese competitors. The dangers of excessive dependence on Chinese production bases have been evident for some time. They came into stronger focus with China's 2010 rare earths embargo, the U.S.-China trade dispute and the COVID-19 disruptions. In 2020, Japan began to subsidize its companies' transfer of production from China to either Japan or to alternative suppliers with lower labor costs. For Japanese companies, this often means building more secure supply chains outside China to serve non-Chinese markets. Such parallel supply chains need not entirely replace exports from China, but they must be big enough to deter China from holding non-Chinese markets hostage.

Indian supply chains for the domestic and export markets have become highly dependent on Chinese suppliers. "China's share of imports into India in 2018 (considering the top 20 items supplied by China) stood

at 14.5%," according to The Hindu newspaper. "In areas such as active pharmaceutical ingredients for medicines such as paracetamol, India is fully dependent on China. In electronics, China accounts for 45% of India's imports."

While border disputes, memories of China's 1962 attack on India and China's long-standing support for India's rival Pakistan are long-term pressures weighing against excessive dependence on China, Indian policymakers were shocked in 2020 by COVID-19 supply chain disruptions and an India-China border incident that killed 20 Indian Soldiers. The result was a fundamental realignment of Indian economic policy toward China. In addition to excluding Huawei and other Chinese telecom suppliers, India banned many popular Chinese apps to "clean" spying and disruption risks to its critical infrastructure. Given the weakest-link character of much critical infrastructure, restrictions on Chinese suppliers and services must be far-reaching to be effective. Due to the high initial dependence of much of Indian industry on Chinese suppliers, however, the kind of abrupt break that occurred in critical infrastructure is not possible in supply chains.

In 2020, the Indian government announced broad subsidies for incremental sales increases from domestic production across 10 major industries. The subsidies target production in areas of heavy dependence on China where



India also has comparative advantage. Such investments not only serve the domestic market but also promise to expand export markets. Such prospects attract investment from both Indian companies and foreign multinationals. Where India is at a comparative disadvantage, suppliers can be diversified to reduce dependence on China.

For many years, Australia's economic growth has rested largely on supplying China's voracious demand for food and raw materials. Then, in the COVID-19 era, Australia received a harsh lesson in the perils of excessive economic dependence on China. By calling publicly for an international investigation of the pandemic's origin, the Australian government touched a nerve. The CCP decided to make Australia an example for the rest of the world of what comes from such public defiance. Chinese diplomats immediately threatened economic sanctions. The editor of China's state-run Global Times tabloid was more colorful: "Australia is always there, making trouble," he wrote. "It is a bit like chewing gum stuck on the sole of China's shoes. Sometimes you have to find a stone to rub it off." China proceeded to impose tariffs and other restrictions on imports of Australian barley, beef, lamb, sugar, wine, lobsters, cotton, timber and coal.

Yet China was not able to impose a high cost on Australia because food and raw materials exporters usually found other buyers. In 2020, the Australian government responded with a plan to subsidize manufacturing for the defense industrial base and in areas of comparative advantage, and to address supply chain vulnerabilities by increasing domestic production and finding more reliable foreign suppliers.

Zooming back out from these three examples, the advantages to coordinating efforts are not hard to see. India's population is roughly the same as China's, and India has the potential to continue growing into an economic and military peer competitor. In narrower economic terms, India has comparative advantage in labor-intensive manufactured goods and in human capital-intensive, high-tech industries such as pharmaceuticals and software. Japan has comparative advantage in a variety of capital-intensive manufacturing sectors, and Australia has comparative advantage in many important foodstuffs and raw materials. Thus, each state has an incentive to reach out to the others for more reliable suppliers and export markets. Thus, each state has an incentive to reach out

to the others for more reliable suppliers and export markets. This high economic complementarity takes on an even more reliable prospect in view of the shared military threats from China; and existing ties have enhanced potential to grow due to the strong capacities

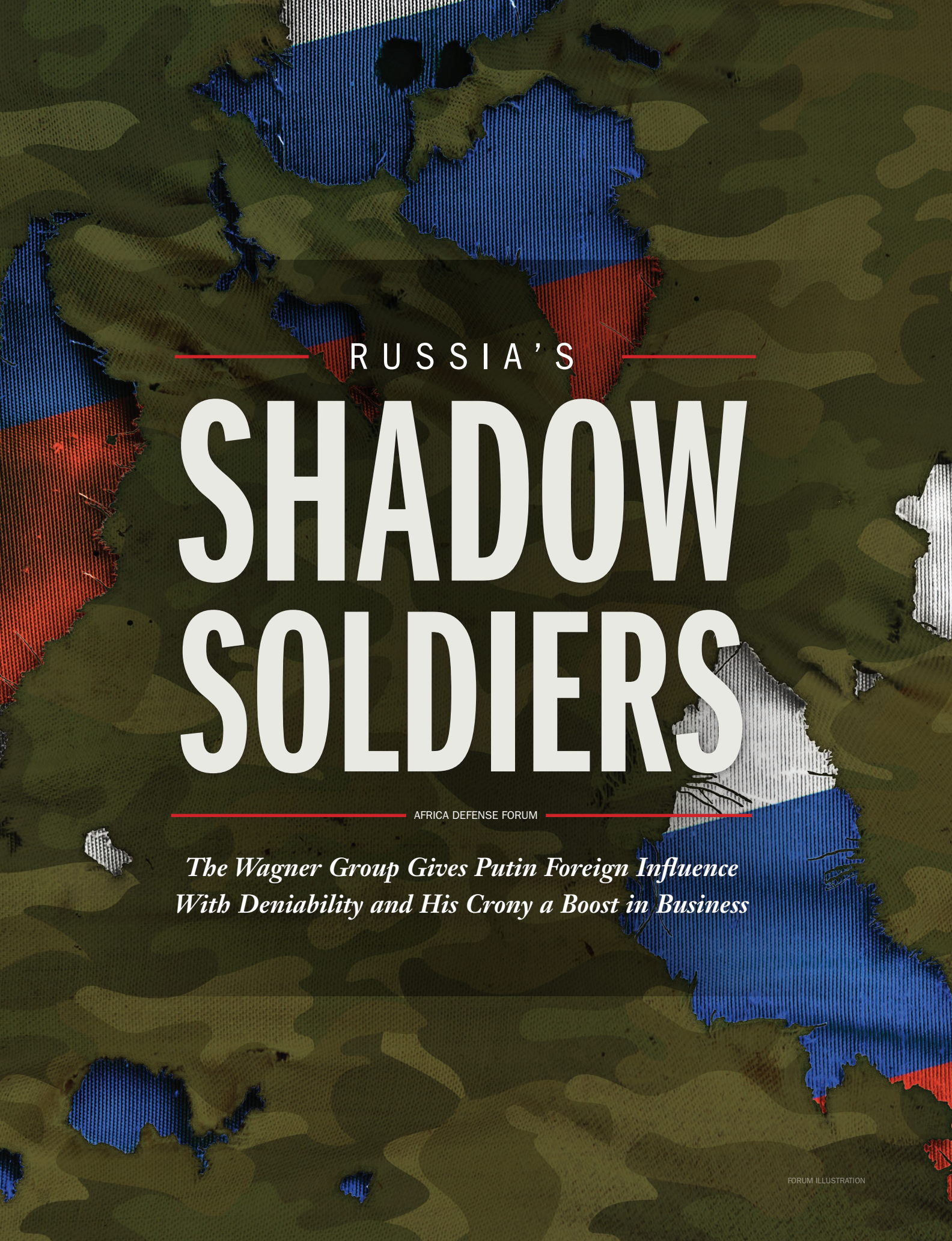


**In 2020, the Australian government responded to Chinese tariffs on exports such as beef, seen here in a Beijing supermarket, with a plan to subsidize manufacturing for the defense industrial base and in areas of comparative advantage.** THE ASSOCIATED PRESS

of the three states. Going forward, it is important for the U.S. and its allies and partners to join these efforts with greater energy. The Quad nations possess a much larger joint market than China's. Given the interest of important regional actors such as Canada, South Korea, Taiwan and many Southeast Asian countries in establishing supply chains and export markets not subject to pressure or disruption from China, the de facto joint market is potentially far larger. The United Kingdom and most EU states also share such interests.

This joint market offers an alternative core for the world economy that is more hospitable and promising than the one dominated by China. Relative to China, the alternative core states generally forgo leverage by their different normative approaches to international relations, which prevent them from routinely using China-style threats or sanctions against other states. But this restraint carries its own strengths. It makes their larger joint markets a more secure base for supply chains that export to the world market, and it offers more reliable, nondiscriminatory market access and more secure protection of intellectual property. □





RUSSIA'S

# SHADOW SOLDIERS

AFRICA DEFENSE FORUM

*The Wagner Group Gives Putin Foreign Influence  
With Deniability and His Crony a Boost in Business*



**I**n Russia's frenzied attempt to flex its muscles, get access to natural resources and increase its geopolitical relevance, it relies heavily on private military companies (PMCs). This strategy produces a small foreign footprint and offers the Kremlin plausible deniability while enriching a small circle of people.

President Vladimir Putin's Russia favors the use of PMCs such as the Wagner Group when forging training and security deals with African nations while positioning itself to access mines and other rich resource repositories.

"They act as force multipliers, arms merchants, trainers of local military and security personnel, and political consultants," according to the Carnegie Endowment for International Peace article, "Implausible Deniability: Russia's Private Military Companies," by senior fellow Paul Stronski. "Nominally private actors, they extend the Kremlin's geopolitical reach and advance its interests. Versatile, cheap, and deniable, they are the perfect instrument for a declining superpower eager to assert itself without taking too many risks."

The Chinese Communist Party (CCP) deploys similar tactics, using Chinese PMCs in Africa and elsewhere to protect CCP assets. The journal *Eurasia Review* referred to Chinese PMCs as "Chinese muscle" that's often found alongside "Chinese money." Put another way, these private Chinese security firms tend to be more prevalent in areas where the People's Republic of China is expanding its One Belt, One Road infrastructure scheme and in host nations where Chinese companies are constructing projects through predatory lending practices, according to experts. "Internationally, the Chinese PMSC [private military and security companies] footprint, while smaller than some others, is growing in size and importance," according to a July 2020 analysis by *Eurasia Review*. (See "Chinese Muscle" sidebar on page 54 to read more about Chinese PMSCs.)

The Wagner Group, the most prominent of Russia's PMCs, emerged from conflict in the Ukraine in 2014, starting with about 250 men and growing to 10 times as many, according to a September 2020 paper by researcher Sergey Sukhankin. They were sent to Syria, where they supported President Bashar Assad's forces and have since made their way into Africa.

"Aside from in Ukraine, Syria and Libya, the Wagner Group has appeared in countries of Sub-Saharan Africa as a 'shadow facet' of the military-technical cooperation between Russia and local states," Sukhankin wrote in "Russian Private Military Contractors in Sub-Saharan Africa: Strengths, Limitations and Implications" for the *Institut français des relations internationales*.

Despite denials and obfuscation from official Russian government sources, observers generally

agree that the Wagner Group is a proxy arm of the government with connections to the national security apparatus, Putin's rich cronies and the president himself. However, successfully documenting these connections can be challenging.

Even so, Wagner forces have been known to operate in a number of African nations, including the Central African Republic (CAR), Libya, Madagascar, Mozambique and Sudan. Their presence often coincides with the business interests of one of Putin's closest allies, the oligarch Yevgeny Prigozhin.



**Businessman Yevgeny Prigozhin, right, shows his school lunch factory to then-Russian Prime Minister Vladimir Putin outside St. Petersburg in 2010.** AFP/GETTY IMAGES

## PUTIN'S CHEF

Despite his close association with Putin, Prigozhin did not start the Wagner Group. That credit falls to Dmitry Utkin, a veteran of the Chechen wars and a former member of the Russian intelligence service known as the GRU.

Utkin worked for the Moran Security Group in Syria, quitting in 2014 to found Wagner, so named for his former call sign, "Vagner." It was a nod to the German composer Richard Wagner, whose works Hitler appropriated for the Third Reich.

Although not a company founder, Prigozhin's influence is said to be key in how the group's forces are employed. Prigozhin's personal history is an extraordinary one: A Soviet court convicted him of robbery and other offenses, and he served nine years in prison. Once released, he hawked hot dogs from a kiosk and eventually opened a restaurant on a docked boat. After serving a meal to Putin there, Prigozhin found favor with the Russian leader and soon was catering Kremlin affairs, becoming known as "Putin's chef."





**Russian President Vladimir Putin, left, shakes hands with Central African Republic President Faustin-Archange Touadera during a meeting on the sidelines of the Russia-Africa Summit in Sochi, Russia, in October 2019.** REUTERS

As Russia transitioned out of its Soviet past and into newfound capitalist ventures in the 1990s, Prigozhin opened St. Petersburg's first grocery store chain, and soon luxury restaurants, according to a report from Turkish news service TRT World.

Prigozhin eventually was drawn into Putin's inner circle, where he found lucrative high-dollar military and school catering contracts. Soon, he had turned his business toward construction and a range of other interests. Often his interests and those of the Kremlin found common ground in places as far-ranging as Syria, Libya and Sub-Saharan Africa.

"Simply put, the company's presence in geopolitical hotspots illuminates coordination between Prigozhin's commercial ambitions and the Kremlin's pursuit of its national interests," Aruuke Uran Kyzy of TRT World Research Centre wrote.

### EXTENDING PUTIN'S REACH

What could a small, private security company possibly do to advance Russian geopolitical aims in Africa and elsewhere?

Perhaps the most valuable asset the Wagner Group offers Putin is plausible deniability. Russia's

constitution reserves all defense and security functions for the government, so establishing PMCs is illegal. However, loopholes allow registering companies abroad and state-run enterprises to have private security forces. In Wagner's case, there's no evidence that it is registered anywhere.




Putin's deployment of Wagner outside Russia gives him and his government influence in other nations without the publicity and liability that comes with national military interventions.

For example: If Wagner is deployed in a conflict in an African country and suffers embarrassing losses, as happened while fighting Islamist militants in northern Mozambique, the Russian government does not have to endure the public fallout associated with losing national military troops during an ill-fated adventure on foreign soil.

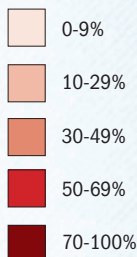
Russian personnel arrived in Mozambique as the two countries forged agreements that will give Russian

# RUSSIA IN AFRICA

## Russian Military Presence in Africa

-  Military cooperation agreement with Russia
-  Proposed logistics base
-  Russian mercenaries





### Percent of country's arms imports supplied by Russia (2009-2018)

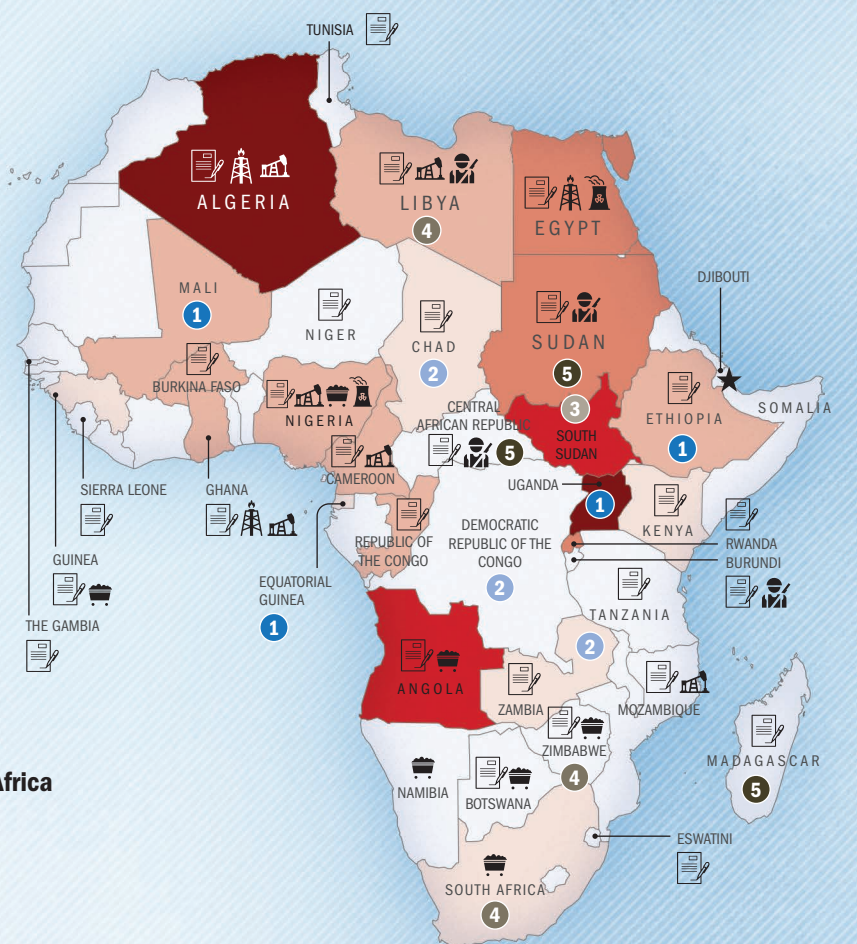


## Russian Influence Operations in Africa



## Russian Energy and Mining Activity in Africa

-  Gas exploration/extraction
-  Oil exploration/extraction
-  Mining
-  Agreement to construct a nuclear power station



Source: European Parliamentary Research Service

FORUM ILLUSTRATION

businesses access to liquefied natural gas, which is plentiful in the nation's north.

Also plentiful in the north are violent insurgent attacks by a relatively new terrorist group, Ansar al-Sunna, which has aligned itself with the Islamic State group. Well-equipped Wagner forces brought in to help an overmatched military soon took significant and embarrassing losses due to their ignorance of the local terrain and their inability to effectively communicate with government forces. They soon departed.

Although the Mozambique engagement went poorly, Wagner personnel tend to be battle-hardened fighters as opposed to retirees or veterans. This provides a ready-made fighting force that allows the Russian government to pursue its foreign policy aims without leaving fingerprints.

Perhaps not surprisingly, Wagner's presence often ends up aligning with Prigozhin's business interests. His Evro Polis energy company entered into a contract with Syria's state-owned General Petroleum Corp. The Associated Press reported in December 2017 that the contract guaranteed Evro Polis 25% of proceeds from oil and gas production at fields its contractors take and protect from the Islamic State group.

"Similarly, as Russia increases its involvement in Africa, Wagner operations have expanded across the continent, where it protects Prigozhin's investments," wrote Alexander Rabin for the Foreign Policy Research Institute in 2019.

In 2017 and 2018, Prigozhin's personal plane was found to have headed to African countries numerous times. Trips included Angola, the CAR, the Democratic Republic of the Congo, Guinea, Guinea-Bissau, Libya, Madagascar, Mozambique, Sudan and Zimbabwe, according to Sukhankin's January 2020 Jamestown Foundation report, "The 'Hybrid' Role of Russian Mercenaries, PMCs and Irregulars in Moscow's Scramble for Africa."

The report notes that all these countries hold three things in common:

- Each is known for social and political instability.
- All are "handsomely endowed with strategically important natural resources."
- Each used to be part of the influence spheres of colonial powers such as Belgium, France and Portugal — nations that Russia no longer considers capable of fending off its involvement in the countries.



# CHINESE MUSCLE

Protecting CCP assets with private military and security companies FORUM STAFF

**R**eferred to by some analysts as “Chinese muscle,” Chinese private military and security companies (PMSCs) are controlled by the Chinese Communist Party (CCP) and assigned to protect assets that include One Belt, One Road (OBOR) infrastructure projects and the Chinese citizens building them.

Since CCP General Secretary Xi Jinping announced OBOR in 2013, it has expanded to more than 80 countries in Central, South and Southeast Asia, the Middle East and the Horn of Africa, according to the journal *Eurasia Review*. As China’s global footprint expands through geoeconomics and geostrategic efforts, so will its dependence on PMSCs.

Additionally, an uptick in crimes against Chinese citizens abroad, including abductions, killings and piracy, has caused concern for Beijing over the past decade, according to the website *Modern Diplomacy*. The use of military resources would seem excessive in most cases, particularly as China already faces criticism for aggressive expansionism, *Modern Diplomacy* reported. The Chinese government has therefore chosen the softer alternative of contracting private security through China-based firms.

“Though Beijing would like to rely upon local forces to provide security, host government authorities may be unable or unwilling to provide Chinese workers and businesses with adequate protection,” according to *Eurasia Review*.

The 2009 Regulation on the Administration of Security and Guarding Services legalized the

use of private security companies (PSCs) in China. By 2013, the number of private security companies operating domestically had risen to 4,000, employing more than 4.3 million security personnel; by 2017, that number had increased to 5,000 companies, according to Meia Nouwens, a senior fellow for Chinese defense policy and military modernization at the International Institute for Strategic Studies.

“Due to the special conditions under which Chinese PSCs emerged and operate, the services they can provide are still substantially different from those offered by their international counterparts,” Nouwens wrote in a 2019 analysis about Chinese private security firms and OBOR. “Their employees are relatively young, lack experience in combat scenarios, and do not normally carry or use arms when operating abroad, even though PSCs are staffed by People’s Liberation Army veterans.”

The use of Chinese PSCs to secure Chinese investments abroad supports Xi’s intent to keep Chinese money within China’s economy, according to the online news magazine *The Diplomat*. Another advantage to China is that its citizens are more likely to protect state secrets and preserve business confidentiality, *The Diplomat* reported.

The footprint of Chinese PMSCs remains relatively small abroad, and Chinese law prohibits them from using weapons outside China, Alessandro Arduino, author of the book “China’s Private Army: Protecting the New Silk Road,” wrote for *The Diplomat*. Still, questions remain about their operation.

“Two important questions are therefore: when does the number of Chinese personnel in a foreign country become one too many? And will the Chinese law on firearms be changed in favor of allowing PSCs to project more assertive power?” Arduino wrote.

Other questions yet to be answered, according to Arduino, include whether the Chinese PSCs will take orders from the government and whether Beijing is going to frame a clear code of conduct and related rules of engagement.

---

*In 2018, three Russian journalists were murdered while investigating the entry of Wagner Group forces into the CAR from neighboring Sudan, where Wagner had been training local security forces.*

---

Corruption and insider deals soon follow lines similar to those in Syria, according to Sukhankin: Moscow secretly strikes a bilateral deal with the nation’s leaders and offers military and security support in exchange for natural resource concessions.

“Under this scheme, a portion of the profits allegedly go to the Russian state budget (via the companies/corporations involved), while the rest is distributed among private individuals who, in fact, may be closely associated with the government,” Sukhankin wrote.

After rumors in late 2017 that Russian mercenaries had been sent to the CAR and Sudan, two companies connected to Prigozhin — Lobaye Invest and M-Invest — won licenses to extract gold, diamonds, uranium and more, Sukhankin wrote. Reports also indicate that Wagner personnel

provide a security detail for CAR President Faustin-Archange Touadera and guard gold mines.

In 2018, three Russian journalists were murdered while investigating the entry of Wagner Group forces into the CAR from neighboring Sudan, where Wagner had been training local security forces. By 2019, talk had turned to the potential for a Russian base in the CAR.

On the surface, the CAR would seem to be an unlikely target for Russian presence and influence. However, the nation's longstanding instability — and its rich deposits of diamonds, gold, uranium and oil — make it a desirable center of influence for Russia. Putin deftly exploited the situation there by relying on a Cold War Soviet-era model that relies on “military-technical cooperation,” according to an analysis by the Jamestown Foundation. The CAR and Russia signed an agreement in August 2018 and the Kremlin has since expanded its footprint in the country using two methods.

First, a military training/consulting agreement began in March 2018 with the arrival of advisors consisting of five military personnel and 170 “civilian instructors,” according to the foundation. Despite statements to the contrary, these instructors are in fact Wagner forces.

Second, Russia has given the CAR's government military and technical equipment to include weapons, ammunition and military vehicles. Most of this assistance is rendered cheaply, as much of the equipment is dated. Also, Russia's goals tilt more toward economic benefits than ideology, according to Jamestown.

Despite this alleged assistance, there is evidence that Russia may be using Wagner to play both sides in the CAR.

For example, Geopolitical Monitor noted in August 2020 that more than 80% of the country remained under rebel control. “Wagner, along with providing military training, allegedly collaborates with these rebels to exploit the local population,” Daniel Sixto wrote. “Wagner forces reportedly coordinated with rebel forces to allow a Russian mining company to access diamond mines in insurgent territory, undermining their wider objective in the region.”

In Libya, Russia has used Wagner to intervene in the conflict there on the side of Gen. Khalifa Haftar against the United Nations-recognized Government of National Accord, which preceded the interim government under Abdul Hamid Dbeibah, known as the Government of National Unity. Libya also is rich in oil deposits, and its Mediterranean coast makes it a highly strategic potential sphere of influence.

U.S. Africa Command has accused Wagner forces of planting mines and other explosive devices in Libya, sometimes hiding them in toys, according to Business Insider.



**People mourn at a Moscow funeral for one of three Russian journalists killed while investigating the Wagner Group in the Central African Republic.** REUTERS

Wagner and Prigozhin also extend influence into the online realm. Reports indicate that Wagner is behind online influence campaigns in Libya that target citizens and bolster Haftar and Saif al-Islam Gadhafi, the son of Libya's late dictator. Similarly, the group is known to have tried to influence the 2018 elections in Madagascar.

Wagner isn't just an advantage for Putin, Prigozhin or the Russian government. Those working abroad for Wagner also benefit, most notably financially. According to TRT World, Wagner personnel can earn 1 million rubles over three months — the equivalent of up to U.S. \$16,000. That can be up to 10 times what they would make as a Russian soldier. Wagner commanders can earn up to three times more. The surviving family of fighters killed in action can get about U.S. \$56,000.

“Wagner is deployed by Russia as an extension of its foreign and military ambitions, and authoritarian regimes just so happen to be the clients,” Ahmed Hassan, CEO of intelligence consultancy Grey Dynamics, told Business Insider. “Of course, those type of regimes often try to solve civil unrest by force, and Wagner is such a tool.” □

A version of this article appeared in Volume 14, Issue 3, of *Africa Defense Forum*, a publication of U.S. Africa Command.



# Battling Human Trafficking in the Bay of Bengal

## BIMSTEC Countries Commit to Fight Exploitation of Women and Children

STORY BY ANASUA BASU RAY CHAUDHURY/OBSERVER RESEARCH FOUNDATION  
PHOTOS BY AFP/GETTY IMAGES

Increased trafficking of people — in particular of women and children — is an urgent concern for the countries of the Bay of Bengal Initiative for Multi-Sectoral Technical and Economic Cooperation (BIMSTEC). Authorities agree that the routes, methods and activities of traffickers have become highly organized, with crime syndicates having a greater degree of infiltration both within and outside the Bay of Bengal region. Most of the victims across the world are female — mainly adult women, but also increasingly girls.

The situation in the Bay of Bengal region is no different. The alarming numbers of women and children being trafficked for forced labor or slavery-like practices (including commercial sexual exploitation) is a crucial concern. Statistics are limited and contested, making it difficult to create an exhaustive map of the situation. BIMSTEC member states include Bangladesh, Bhutan, India, Myanmar, Nepal, Sri Lanka and Thailand.

Nonetheless, available data has drawn BIMSTEC's attention. This analysis provides an overview of the trafficking of women in the Bay of Bengal region, particularly around Bangladesh, India and Nepal, a contiguous zone and a hub of this type of organized, transnational crime.

The data reveals how trafficking is related to forced migration and raises several key questions: How do women and children fall prey to trafficking? What cross-border legal mechanisms exist within the Bay



region? What is BIMSTEC's response as a subregional organization?

### SETTING THE TONE

The United Nations adopted the Trafficking in Persons Protocol in November 2000, which became enforceable in December 2003. It defines trafficking as “the recruitment, transportation, transfer, harboring or receipt of persons, by means of the threat or use of force or other forms of coercion, of abduction, of fraud, or deception, of the abuse of power or of a position of vulnerability or of the giving or receiving of payments or benefits to achieve the consent of a person having control over another person, for the purpose of exploitation.”





Exploitation includes different forms of sexual exploitation, forced labor or services, slavery or practices similar to slavery, servitude or the removal of organs for sale. Trafficking in persons is a multidimensional phenomenon including social, economic and criminal factors, gender, health, migration and development, according to the Global Alliance Against Traffic in Women report, "Collateral Damage: The Impact of Anti-Trafficking Measures on Human Rights around the World."

In the past decade alone, there has been an upward trend in the number of victims identified and traffickers convicted globally,

according to the "Global Report on Trafficking in Persons 2018" by the U.N. Office on Drugs and Crime (UNODC). There is a dearth of data on human trafficking specifically in the Bay of Bengal region. Nonetheless, the UNODC report can be used to understand the situation in South and East Asia. Of the total trafficked people in South Asia, females account for 59% and males 41%, according to the report. Of all incidents, trafficking for sexual exploitation (50%) is nearly equal to trafficking for forced labor (49%).

In 2016, 67% of the total reported victims of trafficking in East Asia and the Pacific were

Photographs of missing Indian children are displayed at a police station in New Delhi.



women. About 60% of these victims were trafficked for sexual exploitation and 38% for forced labor. In Myanmar, most of the victims were women. In Thailand, there was more trafficking of people for forced labor than for sexual exploitation, and men accounted for most of the victims. Both these countries reported particularly high numbers of women being convicted of trading in humans. The vast majority of convicted traffickers are citizens of the country of conviction.

South Asia is the origin area for a significant proportion of humans trafficked to the rest of the world, according to the UNODC report. Victims from South Asia have been detected in more than 40 countries. The main destinations are in the Middle East. To a lesser extent, victims have been reported in Western and Southern Europe and in North America. Victims from South Asia — particularly Bangladesh and India — also end up in Southeast Asia.

Meanwhile, the diversity of the flows and the number of victims detected indicate that human trafficking from East Asia is of a global dimension. The flows from the region to North America, the Middle East and Western and Central Europe are particularly relevant. Thailand is a destination for victims trafficked from Cambodia, Laos, Myanmar and Vietnam.

### **SPOTLIGHT ON BANGLADESH-INDIA-NEPAL ZONE**

Based on the regional patterns of human trafficking, analysts and authorities categorize some countries as sites of origin and others as destinations. However, the situation on the ground is more complex. India, for instance, is not only a destination but a transit country as well. It's an intermediary space, from where women and children are trafficked within the region as well as globally. Bangladesh and Nepal, meanwhile, can be characterized purely as sites of origin.

A 2008 report revealed that Bangladesh and Nepal were two of the biggest suppliers of the traffic into India, accounting for 2.17% and 2.6%, respectively. A report by Justice and Care, in association with the Indian Border Security Force, found that more than 500,000 Bangladeshi women and children ages 12 to 30 were sent to India illegally in the past decade. Nearly 35,000 Nepalis (15,000 men, 15,000 women and 5,000 children) were trafficked into India from 2018 to 2019, according to a report by the National Human Rights Commission.

Nongovernmental organizations (NGOs) battling trafficking estimate that about 50 women are traded from Nepal to India every day. Nepalese victims of forced labor trafficking often are transported through Myanmar and Sri Lanka to their final destination. Hundreds of thousands of Rohingyas have fled from Rakhine in Myanmar to neighboring Bangladesh, according to the U.S. State Department. Among these refugees, a substantial number of women and girls have been traded for sex work in Bangladesh and India.

Traffickers abduct Rohingya women and children who

are in transit as well as those already in refugee camps in Bangladesh and sell them into forced marriages in India, Indonesia and Malaysia. Some victims reportedly also have been subjected to forced labor or sex trafficking.

Traffickers transport Rohingya girls within Bangladesh to Chittagong and Dhaka and transnationally to Kathmandu, Nepal, and Kolkata, India, for sex work; some traffickers also trade these girls over the internet. Once victims are trafficked to another country, they lose their rights and become virtually stateless. Some start as migrant workers but end up in brothels, primarily because there are no authorized safe channels for female migrant workers to guarantee their employment, let alone be paid for their work.

In most cases, the migration occurs without legal or authorized documents. Unskilled female workers ages 9 to 25 constitute the most vulnerable group in human trafficking. A U.N. report on trafficking in women, written by Sri Lankan lawyer and human rights advocate Radhika Coomaraswamy, provided important indicators for the possible intersections between trafficking and migration. The growth in migration and trafficking flows has resulted from a combination of factors. Illiteracy, poverty, class clashes, natural calamities and political and ethnic unrest have contributed to heightening the vulnerabilities of marginalized groups, making them even more susceptible to gross violations of human rights.

### **CROSS-BORDER LEGAL MECHANISMS**

Until recently, the national governments of the BIMSTEC members did not prioritize the issue of cross-border human trafficking. However, most of the region has now committed at the national level to combat the trafficking of women and children. Bangladesh, India and Nepal are perhaps the most proactive in attempting to combat the problem through the passage of national legislation. However, domestic laws face issues of implementation and enforcement; impunity still prevails despite the legislation.

#### **• Bilateral Responses**

The Bangladesh-India memorandum of understanding signed in 2015 was a significant move in their efforts to prevent human trafficking. It has focused on three aspects: expansion of the definition of trafficked individuals; repatriation; and the creation of a joint task force. India has been planning to sign similar agreements with other neighbors, such as Myanmar and Nepal.

In November 2019, the Union Cabinet of India approved an agreement with Myanmar on bilateral cooperation for the prevention of trafficking in persons, covering rescue, recovery, repatriation and reintegration of victims. In Thailand, agencies including the Ministry of Social Development and Human Security, the Royal Thai Police, the Immigration Bureau, the Office of the Attorney General and the Office of the Judiciary have cooperated with the Myanmar police and other agencies

to assist and expedite the repatriation of Myanmar victims through the reception center in Myawaddy near the Myanmar-Thai border.

#### • SAARC's Approach

The signing of the Convention on Trafficking in 2002 by the South Asian Association for Regional Cooperation was a landmark step toward recognizing the importance of issues relating to cross-border human trafficking and undocumented migration. However, despite being regarded as a milestone in coordinating interventions against human trade at the regional level, the convention has its limitations. For one, it defines trafficking within the limited scope of prostitution. This definition needs to be broadened.

#### • BIMSTEC's Role

BIMSTEC has identified the fight against terrorism and organized international crime as one of the most important prerequisites for sustainable growth and for maintaining peace in the region. At the eighth Ministerial Meeting held in Dhaka in December 2005, BIMSTEC added a priority sector of counterterrorism and transnational crime, with India as the lead. Accordingly, a joint working group was formed, including four subgroups, each with a lead country: intelligence sharing (Sri Lanka), financing of terrorism

(Thailand), legal and law enforcement issues (India), and prevention of trafficking in narcotics and psychotropic substances (Myanmar). It's unclear how the February 2021 military coup in Myanmar will affect that nation's role in anti-trafficking efforts.

In 2009, the BIMSTEC Convention on Cooperation in Combating International Terrorism, Transnational Organized Crime and Illicit Drug Trafficking was adopted. Comprising 15 articles, the convention can be considered a confidence-building measure, and the member states, subject to their domestic laws and regulations, made a commitment to cooperate in combating international terrorism, transnational organized crime and illicit trafficking in narcotic drugs and psychotropic substances, including their precursor chemicals. However, the convention does not mention human trafficking or undocumented migration.

All member states have ratified the convention except Bhutan. In principle, Bhutan agrees with the agenda of combating human trafficking. A lack of clarity remains about the nature of the extradition treaty at the BIMSTEC level because Bhutan has already signed a bilateral extradition treaty with India.

#### RECOMMENDATIONS

BIMSTEC has yet to take collective measures to stop the trafficking of its people within its borders. In relation



A Nepalese police officer monitors vehicles for women and girls who may be victims of human trafficking.



to the countries' populations, the response level of criminal justice appears to be limited. For instance, in 2016, countries in South Asia reported lower conviction rates compared to those in more populated regions; the situation is similar in BIMSTEC.

While significant milestones have been achieved by national governments in introducing anti-trafficking initiatives in the Bay region, the criminal activity continues unchecked. Crossing national borders is a daily routine for many; thus, the role of security officials at border checkpoints is crucial. The risks of, and possible responses to, trafficking could be disseminated as practical information and should be provided to refugees, internally displaced people and communities along migration routes.

Indeed, the international community's role is important in facilitating anti-trafficking strategies. In this context, the 2018 UNODC report recommended that the international community "accelerate progress to build capacities and cooperation, to stop human trafficking especially in conflict situations and in all our societies where this terrible crime continues to operate in the shadows." The report indicated that in precarious socioeconomic conditions or situations involving persecution, people escaping conflict are compelled to

- **A More Holistic View**

Under the ambit of the counterterrorism and transnational crime sector of BIMSTEC, more focused and coordinated efforts should be adopted to tackle all interconnected segments of human trafficking. The definition of human trafficking must be considered in a more holistic manner, incorporating the various facets of cross-border undocumented migration.

For possible cross-border cooperation, member states must strengthen infrastructural and institutional connectivity, enhancing counterterrorism and transnational crime measures through the convergence of rules, regulations and policies.

- **An Understanding of Victims' Perspectives**

While trafficking for sexual exploitation may be carried out by criminals using physical violence and other coercive methods, victims may also be trapped in such situations by abuse and deception. Institutions dealing with human trafficking should collaborate to identify the often complex contexts and realities in which sexual exploitation takes place in order to respond to victims' physical, psychological, social and economic needs.



Suspects sit in custody, accused of smuggling Rohingya migrants into Indonesia. Boatloads of Rohingya fleeing Myanmar are victims of a multimillion-dollar international human trafficking network.

migrate, accepting fraudulent job offers in neighboring countries or fraudulent marriage proposals that bring them to exploitative situations. Further, the report noted, "armed conflicts tend to have a negative impact on the livelihood of people living in the surrounding areas, even when they are not directly involved in the violence. Again, traffickers may target communities that are particularly vulnerable because of forced displacement, lack of access to opportunities for income generation, discrimination and family separation."

This analysis offers the following recommendations to arrest the incidence of human trafficking in the BIMSTEC region:

- **Free Exchange of Information**

Because of the transnational nature of this organized crime, it is important to have free and fair exchange of information among member states. In most cases, victim data is not systematically collected. As most countries in the Bay region are parties to the U.N. Trafficking in Persons Protocol and have appropriate laws in place, it is time to focus on the implementation of the protocol provisions. In the spirit of shared responsibility and international cooperation, support from neighboring countries affected by these trafficking flows can help accelerate anti-trafficking efforts.





- **Engage NGOs and International Organizations**

While transnational trafficking networks are still prevalent, appropriate responses can be found using international cooperation and national justice measures. Different stakeholders relevant in this field, including NGOs and international organizations, should engage in constant dialogue.

- **Address Gender, Migration and Labor Issues**

The increase in trafficking of women and children in the BIMSTEC region runs parallel to rising illegal and undocumented migration within the region. Economic growth, relative prosperity and peace on the other side of a border act as pull factors. Growing economies create increased demand for imported labor. Young women, in particular, are in demand because they are presumed to be more compliant and less likely to object to substandard working conditions. BIMSTEC should work toward linking issues related to gender, migration and labor.

- **Anti-Trafficking Interventions for Children**

The trafficking of children is an urgent concern. There should be a holistic approach to reduce the vulnerability of children to exploitative patterns. Anti-trafficking interventions for children can be more effective if they are included in programs to

provide quality education for all, especially in settings at an increased risk of trafficking, such as refugee camps.

## CONCLUSION

BIMSTEC is finalizing its charter and rules of law. It would do well to include the issue of human trafficking in its priority agenda. Reliable, updated data is elusive. Still, available data points to a dire situation — especially in the contiguous zone of Bangladesh, India and Nepal — that needs immediate, suitable responses from national governments and BIMSTEC as a collective.

After all, the grouping has identified the fight against terrorism and organized international crime as one of the most important prerequisites for peace in the region. This priority designation necessitates the need for more focused exchange of information among BIMSTEC states and a more holistic view of the spectrum of issues related to trade in humans. □

**Residents of the Shakti Samuha safe house take part in informal education classes in Kathmandu, Nepal. Shakti Samuha, an organization started by trafficking victims, organizes and empowers survivors through legal counsel, vocational training, shelter housing and therapy.**

The Observer Research Foundation originally published this article in November 2020. It has been edited to fit FORUM's format. To access the original report, visit <https://www.orfonline.org/research/strengthening-anti-human-trafficking-mechanisms-in-the-bay-of-bengal-region/>.



---

INTEGRATING

# HUMAN RIGHTS

INTO PEACEKEEPING

---

DR. NAMIE DI RAZZA AND JAKE SHERMAN / INTERNATIONAL PEACE INSTITUTE

---



## U.N. PROMOTES READINESS IN KEY AREAS TO BOLSTER OPERATIONS

To advance reforms aimed at improving the performance and accountability of United Nations peace operations, the U.N. Secretariat and troop- and police-contributing countries (T/PCCs) are expected to strengthen the operational readiness of personnel deployed to the field. This requires ensuring that peacekeepers have the requisite knowledge, expertise, training, equipment and mindset to implement their mandate in accordance with U.N. principles, values, standards and policies.

The operational readiness of uniformed personnel is critical to the effective delivery of mandated tasks authorized by U.N. Security Council resolutions. The U.N. Department of Peace Operations (DPO) and Department of Field Support therefore developed an Operational Readiness Assurance and Performance Improvement Policy, as well as related guidelines, in 2015. Since that policy was created, there has been a gradual recognition of the important role of human rights as part of overall performance. For example, as part of the Action for Peacekeeping Initiative's "Declaration of Shared Commitments," member states and the U.N. Secretariat reaffirmed that peacekeeping operations make an important contribution to protecting civilians and human rights.

They also acknowledged the need to "support pre-deployment preparations of personnel and capabilities required for effective performance, and the existing human rights screening policy." Member states further committed "to certifying that prospective personnel meet U.N. standards for service in U.N. peacekeeping operations."

We seek to define the concept of human rights readiness for peacekeepers, which is intended to complement operational readiness to make peace operations more effective and fit for purpose. In the context of U.N. peace operations, human rights readiness is the extent to which personnel provided by T/PCCs are prepared and willing to cooperate with missions' human rights components and proactively integrate human rights into planning and operations, including for the implementation of protection of civilian mandates.

Building on existing U.N. policy frameworks, standards and initiatives, such readiness encompasses the obligations of these personnel to respect

international humanitarian and human rights law when serving in a peace operation. It also includes their obligation under the U.N. Charter and U.N. policies to promote and advance human rights in their work, as well as the support the U.N. provides to help them meet this obligation.

The human rights readiness of peacekeepers is ensured by T/PCCs and the U.N., which should support and assess that readiness by integrating human rights and humanitarian law into the generation, operational configuration and evaluation of uniformed personnel. This includes incorporating this law into policies, standard operating procedures and mechanisms that guide force generation and predeployment processes — notably with regard to training and equipment requirements and certification, screening and selection processes.




**Nepalese Soldiers stand in formation alongside Soldiers from multiple nations during a global peace operations training exercise led by the Nepal Army.** STAFF SGT. APRIL DAVIS/U.S. ARMY

Human rights readiness also entails putting in place accountability mechanisms, in law and in practice, to ensure that uniformed personnel comply with their human rights obligations. We analyze opportunities and gaps in human rights readiness, exploring ways to improve the human rights readiness of peacekeepers, including their preparedness, ability, capacity and commitment to respect and promote human rights and integrate them into their work on the ground.

---

**Nepalese peacekeepers conduct convoy operations drills with U.S. Marines in Mongolia.** STAFF SGT. BALINDA O'NEAL DRESEL/U.S. ARMY NATIONAL GUARD





An Indian peacekeeper stands guard at a United Nations mobile operating base on the outskirts of Bunagana in the Democratic Republic of the Congo's restive North Kivu province.

AFP/GETTY IMAGES

A comprehensive human rights readiness framework would include mechanisms to integrate human rights considerations into the operational configuration and modus operandi of uniformed personnel before, during and after their deployment. We start the process of developing this framework by focusing on the steps required to prepare and deploy uniformed personnel through force generation, predeployment assessments and training.

### HUMAN RIGHTS IN U.N. PEACEKEEPING

Human rights constitute a core function of U.N. peace operations, regardless of whether missions have an express human rights mandate. Most peace operations, including all multidimensional peacekeeping operations, have a mandate that includes: promoting and protecting human rights through monitoring and investigation; analysis and reporting; capacity building for state institutions, including national human rights institutions, and civil society; early warning; protection of civilians (POC); and support to governments in combating impunity.

Many peace operations are also mandated to protect civilians, an objective that relies on integrated efforts by their military, police and civilian components, including human rights sections. These operations may also have an explicit human rights mandate.

In the context of peace operations, POC refers to protection from threats of physical violence. It is therefore closely linked to human rights work aimed at guaranteeing the right to life and physical integrity

and to the positive obligation to protect people from threats to their right to life and from ill-treatment, as established by human rights law. Protection of civilians is pursued through three tiers: dialogue and engagement, the provision of physical protection and the establishment of a protective environment.

Human rights activities undertaken as part of this work can include investigation and monitoring of abuse, sensitization to international humanitarian law (IHL) and the fight against impunity, all of which contribute to preventing and responding to threats of physical violence against civilians. The U.N. policy on POC is anchored in international law, describing POC mandates as “a manifestation of the international community’s determination to prevent the most serious violations of international humanitarian law, international human rights law and international refugee law and related standards” that “must be implemented in both the letter and spirit of these legal frameworks.”

Close coordination among human rights officers and military and police personnel enables missions to use different types of expertise and their respective tools and comparative advantages to maximize their mission’s impact on POC. Beyond the mission-specific mandates for POC and human rights, all U.N. peace operations and all U.N. personnel are legally obligated to comply with human rights standards and international humanitarian and refugee law and to uphold U.N. human rights principles when implementing their mandates.

The U.N.’s Capstone Doctrine established that “international human rights law is an integral part



of the normative framework for United Nations peacekeeping operations” and affirms that “United Nations peacekeeping personnel — whether military, police or civilian — should ... understand how the implementation of their tasks intersects with human rights.” U.N. policy documents have also consistently reiterated and elaborated on the centrality of human rights to peace operations.

A 2011 U.N. policy governs the integration of human rights into all peace operations, including special political missions and peacekeeping operations. The policy requires missions without human rights mandates to uphold and advance human rights standards and to avoid adversely affecting human rights through the implementation of their mandates. It defines the roles of mission components and sections to advance human rights through their functions.

### HUMAN RIGHTS READINESS IN FORCE GENERATION

In his report on the implementation of the recommendations of the High-Level Independent Panel on Peace Operations, the secretary-general pointed out that “it is essential that United Nations personnel, both civilian and military, conduct themselves in a manner consistent with our values” and that the “human rights record and performance of contributing countries is an

integral part of this.” In line with this, human rights are considered as part of the force generation process, from screening to the selection of personnel. Many efforts have been undertaken to make sure that peacekeepers being deployed have not committed human rights violations. However, the current system mainly focuses on screening out perpetrators through formal policies and processes rather than favoring candidates who have demonstrated their readiness to promote and protect human rights.

The force generation process also entails visits to contributing countries, such as assessment and advisory visits, (optional) operational advisory visits and predeployment visits (PDVs). These visits are intended to ensure the operational readiness of individual military units deployed in U.N. peacekeeping operations. Assessment and advisory visits are conducted before units are formed and focus on verifying a country’s readiness to contribute to peace operations in terms of training and unit-sustainment capabilities. In addition to soldiering abilities, conduct and discipline, including sexual exploitation and abuse, can be part of this assessment.

PDVs for military units, which are led by the U.N. Office of Military Affairs Force Generation Service and include representatives from the Integrated Training Service and the Department of Operational Support’s

**Sri Lankan troops march during a passing out parade in April 2021 before leaving for United Nations peacekeeping duties in Mali.**

AFP/GETTY IMAGES





contingent-owned equipment team, aim to verify the country's capacities and assess its ability to contribute. Most recently, enhanced PDVs have encompassed the validation of military skills, including for the protection of civilians.

To guide these assessments, the Office of Military Affairs has reviewed tasks, conditions and standards related to POC for infantry units in accordance with the revised U.N. Infantry Battalion Manual. Remarkably, the Office of the U.N. High Commissioner for Human Rights (OHCHR) was not part of the discussions regarding the establishment of an operational readiness framework for T/PCCs.

Although human rights are mentioned as one of the parameters of the operational readiness of military units, no human rights experts systematically take part in these advisory and predeployment visits. The visits often focus on training and equipment requirements and amount to box-ticking exercises to formally recognize the processes that T/PCCs have established to comply with operational readiness standards, as defined in the U.N.'s policy. Therefore, they are not necessarily meant to evaluate human rights readiness beyond verifying the existence of a basic training module on human rights during predeployment training. If an in-mission performance evaluation reveals gaps in human rights for a specific unit during its deployment in a peacekeeping mission, this can, in theory, be included in the next predeployment visit and be discussed with the contributing country. In practice, however, the extent to which human rights readiness is considered a critical issue during these assessments remains to be seen.

As recognized by U.N. officials, human rights remains a sensitive issue and there is no clear guidance on how to engage T/PCCs on this, beyond the standard language that appears in diplomatic notes and self-attestation requirements. There is also a strong sense within force generation services that requirements for troop contributing countries, including substantial training and the provision of many documents, are already burdensome. As a result, appetite for another framework on human rights readiness remains limited. Moreover, POC considerations have only recently been expanded in the force and sector commanders' evaluation of units.

### PREDEPLOYMENT TRAINING: A NATIONAL RESPONSIBILITY

Member states are responsible for the predeployment training of military and police personnel assigned to U.N. peacekeeping operations. To assist T/PCCs, the DPO's Integrated Training Service developed and regularly updates standardized training materials, drawing on substantive expertise from across the U.N. system, including from OHCHR. The Integrated Training Service also supports member states in delivering training in two ways: through mobile training teams, which enhance national training capacities,

and through training-of-trainers courses for T/PCC instructors who provide predeployment training to national uniformed personnel.

In modules that include human rights content, OHCHR experts are frequently involved in both types of training, subject to OHCHR's capacity limits. The U.N.'s core predeployment training materials provide a common foundation for all military and police personnel to understand the U.N.'s peacekeeping principles, guidance and policies. These materials encompass generic, specialized and mission-specific elements. They also include modules on the legal framework for U.N. peacekeeping, such as an overview of international human rights law (IHRL) and international humanitarian law (IHL); the duties of U.N. peacekeeping personnel to promote and protect human rights; and mandated tasks pertaining to human rights, including women's and children's rights, and the protection of civilians in U.N. peacekeeping operations.

### DELIVERY GAPS IN PREDEPLOYMENT AND IN-MISSION TRAINING

In the current peacekeeping training regime, much of the focus remains on the normative framework rather than on how to operationally support human rights in missions. The sensitization of uniformed personnel to human rights is often limited to a presentation of human rights norms and legal frameworks. There are only rare opportunities to expand on this sensitization by providing training on how military personnel should integrate human rights into their planning and operations and work with their human rights colleagues in the mission. Without this training, there is a risk that some military personnel could see all human rights issues as the responsibility of human rights sections, diminishing their own sense of responsibility for human rights.

This suggests a disconnect between the normative framework on which peacekeeping is based and human rights-related mandated tasks carried out by the mission, as well as between POC and human rights. Several of the U.N.'s training and human rights staff have acknowledged that existing training practices and methodologies are insufficient, providing uniformed personnel with only a cursory understanding of how IHRL and IHL translate into operational considerations.

Current training does not provide personnel with adequate knowledge of applicable laws, norms and policies, nor does it provide guidance on how uniformed personnel should work with their human rights colleagues. In short, it fails to translate human rights knowledge into daily practice. As the International Committee of the Red Cross (ICRC) has noted, "Adding a few hours on IHL and/or IHRL to the existing training program without modifying its content is far from effective."

Instead, these experts argue that understanding human rights in the context of peacekeeping, and more



**Philippine Soldiers prepare to enter a fictitious United Nations food distribution site during a peacekeeping exercise in Bangladesh.**

MASTER SGT. JON DYER/U.S. AIR FORCE

broadly of POC, requires that it be incorporated into broader training provided by member states to all their military and police, particularly to command and staff officers. Predeployment training is too late in the process to introduce human rights principles and legal concepts to peacekeepers, when much of the focus is often still on ensuring basic soldiering skills. “Historical reflection and social psychology show that the aims of basic training (desensitization, breaking down a soldier’s inculcated reluctance to kill, unit cohesion and obedience to the command chain) are antagonistic to many of the aims of IHL training,” according to the ICRC.

A similar argument can be made for IHRL. IHL and IHRL training needs to be meaningfully integrated into general military and police academy curricula, which is not the standard for a lot of major T/PCCs. This could help personnel develop the correct reflexes through repeated exposure and practice.

### UPHOLDING HUMAN RIGHTS ACROSS MISSIONS

The protection and promotion of human rights have become essential functions of peacekeeping missions since their inclusion in the 1991 mandate of the U.N. Observer Mission in El Salvador. Although human rights components have a critical role in this regard, upholding human rights is a mission-wide responsibility that encompasses not only civilian human rights officers but also military and police components.

The U.N. is facing a moment of increased attention to the operational performance of peacekeeping. The

human rights readiness of U.N. uniformed personnel is a key determinant of this performance, as well as of the U.N.’s credibility and reputation and its commitment to prevention. To professionalize peacekeeping, the U.N. and its member states need to ensure that uniformed personnel understand and have the skills to fulfill their human rights responsibilities and enable the work of human rights components.

Human rights need to be a systematic part of the process of force generation and preparedness, which would also make peacekeeping more accountable to the public and more credible to the U.N.’s partners. Human rights readiness is intended to be a framework against which existing operational requirements related to human rights standards for T/PCCs should be assessed. As with operational readiness, it is a collective effort by T/PCCs and the U.N. Secretariat, which are both involved in all relevant components of peace operations.

To strengthen the human rights readiness of military and police units deployed in U.N. peace operations, tangible action by T/PCCs and the U.N. must take place. This would prepare units to uphold human rights standards and better integrate human rights considerations into their work. It would also ensure that uniformed components can deliver on such a commitment. □

Dr. Namie Di Razza joined the International Peace Institute (IPI) in October 2016 after working on U.N. peace operations and protection of civilians. Jake Sherman is IPI’s senior director for programs and director of the IPI’s Brian Urquhart Center for Peace Operations. This report has been edited to fit FORUM’s format. To read the full report, which IPI published in April 2020, visit <https://www.ipinst.org/2020/04/integrating-human-rights-into-operational-readiness-of-un-peacekeepers>



# WHY IS CHINA RATTLED?

## The Inaugural Quad Leaders Summit Delivered a Clear Message to Beijing

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

**T**he Quadrilateral Security Dialogue (Quad) summit in March 2021 did not name the People's Republic of China (PRC) directly, but Beijing seemed rattled by the event, with its mouthpiece, the Global Times newspaper, speculating that Quad members Australia, India, Japan and the United States were hyping the “China threat” even before the event. Apparently, China saw a major challenge to its dream of a China-centric Indo-Pacific in the Quad's call for a free, open, inclusive and healthy region that is “anchored by democratic values and unconstrained by coercion.” The PRC's hope that the four-country group hasn't formed a cohesive force may need revisiting: Quad leaders attended a summit in September 2021 at the White House and have agreed to pursue important agendas through three focused working groups.

### **BENIGN AGENDA BUT CLEAR MESSAGING**

The Quad's efforts expressed unanimity in the need for a free, open, rules-based order, rooted in international law to advance security and prosperity and to counter threats to the Indo-Pacific and beyond. But the agenda item that attracted global attention was the call for a collective response to the COVID-19 pandemic in terms of synergizing vaccination efforts, with India as a manufacturing hub and assisted by others, to roll out 1 billion vaccines by 2022. The other two working groups focused on emerging critical technologies and climate change.

The agenda seemed benign, but Beijing did not miss the connection in the Quad's first summit to issues such as freedom of navigation and overflight and to concerns about “aggression” and “coercion”

against Quad members by the PRC. No one called out China directly during the summit, but the PRC knows that it challenged the rules-based order by junking the Permanent Court of Arbitration's 2016 ruling dismissing its expansive maritime claims in the South China Sea and that it continues to coerce Indo-Pacific nations. The Chinese response of calling the Quad meeting “selective multilateralism” and “COVID politics” shows its frustration with the emergence of an alternate global vaccination collaboration, something that China sought to unilaterally reserve for itself for profiteering.

The list of shared challenges to be addressed by the Quad includes cyberspace, counterterrorism, quality infrastructure investment, and humanitarian assistance and disaster relief (HADR), some of which entail alleged Chinese involvement, such as cyberattacks and the lack of transparency of the World Health Organization.

The Quad's assertion to support the rule of law, freedom of navigation and overflight, democratic values and territorial integrity has added to the frustration of Beijing, which has started firing propaganda salvos through the Global Times newspaper, calling India a “negative asset” for groups such as BRICS (Brazil, Russia, India, China and South Africa) and the Shanghai Cooperation Organisation and saying that it fails to understand Chinese goodwill.

### **PROBLEMS AND DIVERGENCES**

China wants the world to believe that there are wide divergences in four democracies getting together. As it evolves, however, the Quad seems to be getting over some of those differences. There is much more



**Then-Japanese Prime Minister Yoshihide Suga, above second right, speaks from Tokyo during the March 2021 virtual summit of the leaders of Australia, India, Japan and the United States, a group known as the Quad.**

**Australian Prime Minister Scott Morrison participates from Sydney in the virtual summit with the leaders of India, from left, the United States and Japan in March 2021.**

THE ASSOCIATED PRESS

acceptability regarding divergent definitions and focus areas within the Indo-Pacific, with the Indian focus on the western Indian Ocean touching African and Gulf countries along with other areas of the Indo-Pacific, which remains the focus of all Quad members.

Foundational agreements signed by India and the U.S., such as the Communications Compatibility and Security Agreement and the Basic Exchange and Cooperation Agreement, as well as joint naval exercises, have improved the interoperability of India with other Quad members, operating within the NATO military-alliance framework.

India is the only Quad member that shares a

land border with China, a source of tension for decades. The PRC has done its best to create apprehension among Quad members by keeping China-India relations fluctuating between tension and harmony. After military border standoffs at Doklam and Ladakh, it's quite clear to Indians that China can't be trusted, which has brought relative clarity to the Indian position. The economic entanglement of each Quad member with China necessitates a resilient supply chain, digital and technological ecosystem, with minimal dependence on China.

There has been consensus among Quad



Indian Prime Minister Narendra Modi receives a COVID-19 vaccine in New Delhi in March 2021.

THE ASSOCIATED PRESS

members regarding support for the Association of Southeast Asian Nations' (ASEAN's) centrality in the region, but its inclusion in the Quad's considerations will be debated, given China's influence over ASEAN. Generally, some ASEAN members have occasionally raised a feeble voice against Chinese aggression (the Philippines, Vietnam), expecting world powers to check Chinese adventurism because they find it difficult to stand up against China's might by themselves. This has emboldened China to continue incremental encroachment in the South China Sea and the region. The PRC has always tried to deal with countries on bilateral terms, using its power to its advantage. In its individual engagements with Australia, India, Japan and the U.S., the PRC will continue to aim for weakening the Quad through bilateral concessions.

### **WILL THE QUAD'S EVOLUTION CONTINUE?**

The Quad emerged after the devastating tsunami in the Indian Ocean in 2004 as the Tsunami Core Group, which executed a credible HADR response. The series of multilateral Malabar naval exercises gave the group a sense of interoperability for anti-piracy, HADR and other maritime missions. The Quad members project themselves as committed to an open and transparent network that "will allow people, goods, capital and knowledge to flow freely."

The Quad is yet to acknowledge that it has a role to play in checking Chinese adventurism in the Indo-Pacific or that it could ever operate as a joint military force. In fact, the Quad has chosen to be diplomatic in saying that it is not directed toward any particular country.

China's incremental encroachment



strategy in the South and East China seas and in Ladakh on the disputed India-China border is a serious concern not only to the countries directly affected by overlapping exclusive economic zones (EEZs) or unsettled borders but also to the rest of the world. The PRC continues to convert maritime features and atolls into military bases and expects other nations to accept them as islands, despite China's improper application of the United Nations Convention on the Law of the Sea (UNCLOS) to claim 200 nautical miles of EEZ around the features, thus converting the South China Sea into a "Chinese lake" over a period of time.

The PRC's encroachment threatens freedom of navigation and overflight along global sea lines of communication and may lead to restrictions such as the creation of an air defense identification zone in the South China Sea. Any such action by any country to restrict freedom of navigation and overflight or to violate the rule of law must be challenged in the U.N. Security Council, with the backing of the Quad.

Implementation of the vision of a Free and Open Indo-Pacific on a rules-based, legal framework is needed. All Quad members except the U.S. have ratified UNCLOS; hence, the U.S. needs to do the same to have the moral high ground. The PRC is reasonably confident that neither the U.S. nor any other country will use military force to dismantle its infrastructure in the South China Sea.

The PRC is also increasing its naval capability at an unprecedented pace. In this context, it is necessary for the Quad to strengthen itself beyond the Malabar exercises and to add teeth in the form of maritime capacity-building, further improvement of interoperability and increased capacity to dominate chokepoints sensitive to China. The Quad is not a military alliance, so it will need a formal structure and a secretariat to take it forward.

### THE WAY AHEAD FOR THE QUAD

COVID-19 vaccines will be manufactured in India and financed by Japan and the U.S. with logistical support from Australia. The intention of the Quad to synergize medical, scientific, financial, manufacturing, critical emerging technology and developmental capabilities in the future is a step in the right direction. The sharing of innovative technology and capacity building for



**An Indian Army convoy travels through a mountain pass bordering China in Ladakh, India. India is the only Quadrilateral Security Dialogue member nation bordering China.**

AFP/GETTY IMAGES

climatic challenges will also serve the interest of humanity. If implemented, these measures will certainly make the Quad an effective grouping.

Quad members must continue freedom of navigation and military exercises in the Indo-Pacific, as China continues to do so. If the strategic situation worsens, there may be a need to position a so-called U.N. Maritime Military Observers Group to prevent an accidental triggering of conflict, which is possible in a region with a high density of combat ships on freedom of navigation missions.

The Quad summit did not signal expansion, but the group needs to have flexibility to incorporate like-minded democratic countries, as many would be keen to join the Quad because the Indo-Pacific is becoming the economic center of gravity and the manufacturing hub of the world. The support of other navies, such as those of France, Germany, the United Kingdom and other NATO members, would deter peace spoilers. The Quad in its present form may not be structured to check Chinese adventurism, but it certainly has the potential to become one of the most effective instruments to do so. Chinese reactions indicate that the Quad certainly has put China on notice, without even naming it. □

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. This article originally was published in March 2021 by Financial Express Online. It has been edited to fit FORUM's format.





# CODIFYING WATER AND RESHAPING ORDERS

## PRC AGGRESSION IN EAST, SOUTH CHINA SEAS

DR. NGUYEN THANH TRUNG AND LE NGOC KHANH NGAN

**T**he People's Republic of China's (PRC's) Maritime Traffic Safety Law (MTSL) took effect September 1, 2021, requiring all foreign vessels entering Chinese territorial waters to notify maritime authorities, carry required permits, and submit to Chinese command and supervision.

This comes after the Chinese government passed a law in February 2021 that authorizes the China coast guard (CCG) to use force on foreign vessels infringing on Chinese sovereignty. Both laws have serious implications for the international order. In addition, they infringe upon provisions of the United Nations Convention on the Law of the Sea (UNCLOS) that grants states the right of passage without requiring permission from the coastal state's government.

The PRC's codification of disputed waters has been building up to its current expansive stage for three decades. The 1992 Law on the Territorial Sea and Contiguous Zone also caused angst among states by violating UNCLOS provisions that define the baselines for measuring the territorial sea and other maritime zones. The PRC applied the straight baseline method, connecting basepoints between several islands far from the Chinese coast, and inflated its resulting territorial sea and exclusive economic zone (EEZ), infringing upon the rights of other nations to use those waters as allowed by international law.

Chinese domestic legislation that goes beyond what is allowed by international law creates opportunities to advance the PRC's territorial goals through coercive means — at the expense of the territory and sovereignty of regional states. Article 12 of the coast guard law allows the CCG to protect Chinese sovereignty, maritime interests, artificial islands, and facilities and construction in waters claimed by the PRC. The CCG can also demolish foreign buildings, structures, floating devices constructed on the seas, islands and reefs under its jurisdiction, according to Article 20 of the law.

The MTSL empowers the Chinese Communist Party (CCP) to further control activities in its waters by dictating the categories of foreign vessels that must provide their information when navigating and berthing in pilotage zones. This means the CCP could define

pilotage zones in disputed areas, even within other claimants' EEZs.

The MTSL and coast guard law are more than isolated violations of international law — they serve a broader ambition of bolstering the PRC's claims by using its own judicial processes.

The PRC's approach relies on vaguely defined legal terms to interpret statutes as needed. Article 74 of the coast guard law defines “waters under Chinese jurisdiction” to include “other waters,” a term that likely refers to disputed waters and those the PRC controversially claimed in the 1992 Law on the Territorial Sea. The new maritime law, meanwhile, is ambiguous as to how harshly, broadly or whether the new legislation will be enforced and over what geographic area.

Regionally, the PRC wants to reset the order that has been in place for decades, and its domestic legislation is an important component of its efforts to shape maritime rules and norms. The coast guard law is arguably an imminent threat to countries involved in disputes with the PRC in the East and South China seas. The law strengthens the argument that the PRC wants to establish a legal basis to justify physical confrontation on the seas.

In practice, Beijing has been increasingly adopting an offensive crouch. With its growing economic and military power, the CCP can impose its domestic law on the areas it controls, regardless of whether they are legally within its jurisdiction. With its military expenditure reaching U.S. \$252 billion in 2020, China has turned its naval fleets and disguised militia vessels into behemoths to outclass regional navies and law enforcement agencies. In this context, forcing vessels from smaller nations to comply with the law does not seem a hard task for Beijing, raising alarm among regional states and the rules-based international community.

**Coast guard cutters from Japan and the United States transit the East China Sea in August 2021.**

THE ASSOCIATED PRESS

Dr. Nguyen Thanh Trung is director of the Saigon Center for International Studies (SCIS) at the University of Social Sciences and Humanities, Vietnam National University, in Ho Chi Minh City. Le Ngoc Khanh Ngan is a research fellow at SCIS. This article originally was published September 27, 2021, on the Center for Strategic and International Studies' Asia Maritime Transparency Initiative website. It has been edited to fit FORUM's format.



# BEACH *guidance*



Royal Thai Navy personnel guide a landing craft during a training exercise at Chulaporn camp in Thailand's southern Narathiwat province in March 2021.

Photo by: The Associated Press



# RELEVANT. REVEALING. ONLINE.

[www.ipdefenseforum.com](http://www.ipdefenseforum.com)

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

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



All platforms may not be available at every location.

## FREE MAGAZINE SUBSCRIPTION

FOR A FREE MAGAZINE SUBSCRIPTION:

[www.ipdefenseforum.com/subscribe](http://www.ipdefenseforum.com/subscribe)

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

PLEASE INCLUDE:

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

DOWNLOAD  
OUR APP!



NEW  
CONTENT  
POSTED  
DAILY!

