February 2026

The Indo-Pacific in Transition

Strategy, Competition, and Cooperation

Editor

Dr. Sayuri Romei

Authors

Dr. Pratnashree Basu
Michal Bokša
Dr. Maximilian Ernst
Dr. Eyck Freymann
LCDR Blake Herzinger
Agnieszka Kurzej
Dr. Chris Li
Annes Llwyd
Dr. Iain MacGillivray
Takuma Matsu
Jiro Minier
Natsuki Momiji
Dr. Masatoshi Murakami
CAPT Diana Y. Myers
Dr. Sayaka Shingu
Dr. Bich Tran

G | M | F

G | M | F

About YSF

Funded by and conducted in partnership with the Sasakawa Peace Foundation, the Young Strategists Forum seeks to develop a new generation of strategic thinkers and equip them with the skills to successfully navigate a world in flux. Since the inaugural Young Strategists Forum in March 2012, GMF and SPF have built a vibrant program centred on the theme of the US-Japan alliance and security dynamics in the Indo-Pacific region. Held in Tokyo, the program emphasizes the importance of pursuing purposeful grand strategic objectives through an innovative combination of lectures, a 36- hour simulation exercise, meetings with policy makers, diplomats, senior journalists and leading academics, and a study tour that includes a visit to a military facility. Participants are selected through a competitive process, open to emerging leaders — academics, journalists, policy makers, politicians, business professionals, and military officers — between the ages of 28 and 42, from the United States, Europe, Japan, and other like-minded Asian countries. Since its creation, the Young Strategists Forum has cultivated a vibrant network of emerging foreign policy leaders. 162 individuals have participated in the Young Strategists Forum, many of whom have risen to prominent positions in their respective professions.

About GMF

The German Marshall Fund of the United States (GMF) is a nonpartisan, nonprofit, transatlantic policy organization committed to the idea that the United States and Europe are stronger together. Founded by Guido Goldman in 1972 through a gift from Germany as a tribute to the Marshall Plan, GMF is one of the world's leading international policy institutions that champions democratic values and the transatlantic alliance by strengthening civil society, forging bold and innovative policy ideas, and developing a new generation of leaders to tackle global challenges. GMF delivers hope by upholding the dignity of the individual and defending freedom in the spirit of the Marshall Plan. GMF is headquartered in Washington, DC, with offices in Ankara, Belgrade, Berlin, Brussels, Bucharest, Paris, and Warsaw.

About Sasakawa Peace Foundation

The Sasakawa Peace Foundation (SPF) is a private non-profit organization established in September 1986. It seeks to contribute to the welfare of humanity and the sound development of international community, and thus to world peace, through activities that foster international interaction and cooperation.

Acknowledgments

This report is made possible by the generous support of the Sasakawa Peace Foundation. We extend our sincere thanks to all those who contributed to this publication, including Nancy Mandel and Claire Rosenson for their meticulous editorial work, and Subigya Basnet for his expertise in formatting. Your dedication and efforts are deeply appreciated.

Disclaimer

The views expressed herein are those solely of the authors and do not necessarily reflect the policy positions of GMF. As a nonpartisan and independent research institution, GMF is committed to research integrity and transparency. The essays contained in this edited volume were written in the spring of 2025. As this publication is released in February 2026, any interpretations or conclusions should be viewed in the context of their original timeframe.

Table of Contents

The Indo-Pacific in Transition: Strategy, Competition, and Cooperation

Introduction by Dr. Sayuri Romei

For more than a decade, the German Marshall Fund of the United States (GMF), in partnership with the Sasakawa Peace Foundation, has selected and convened a select group of emerging leaders in national security, foreign policy, and geoeconomics through the Young Strategists Forum (YSF) in Tokyo. The forum brings together a diverse cohort from government, military institutions, think tanks, academia, and the private sector across the United States, Europe, Japan, and the broader Indo-Pacific. Beyond participation in a rigorous tabletop strategy exercise and engagements with senior officials and experts in Japan, the program is designed to foster enduring cross-border relationships among future policymakers and practitioners. Supported by an alumni network that now numbers in the hundreds, the forum strengthens professional ties that underpin long-term cooperation among like-minded countries.

The most recent convening of the YSF took place in Tokyo from January 30 to February 5, 2025. Participants took part in an Indo-Pacific strategy simulation led by Dr. Zack Cooper of the American Enterprise Institute and engaged in discussions with officials and experts from Japan's National Security Secretariat, the Ministry of Defense, leading universities including the University of Tokyo and Keio University, and prominent research institutions such as the Institute of Energy Economics Japan and the Sasakawa Peace Foundation.

This volume brings together essays written by participants in the 2025 forum, offering them a platform to reflect on insights drawn from both their professional experience and their time in Tokyo. Authors were encouraged to pursue topics of greatest relevance to their own interests and expertise. Collectively, these contributions provide a multifaceted examination of the evolving regional and global order, the challenges confronting the United States, Japan, and other like-minded partners, and the avenues through which these countries can work together to defend and advance a free and open international order.

The essays are organized around shared strategic themes shaping the Indo-Pacific. The volume opens with questions of hard security and deterrence. **Agnieszka Kurzej** examines the expanding role of Euro-Atlantic navies in Indo-Pacific security, highlighting

the strategic value of presence, partnership, and interoperability. Building on this focus, **Iain MacGillivray, Masatoshi Murakami, and Maximillian Ernst** analyze the growing convergence of German, Australian, and Japanese deterrence strategies, demonstrating how these geographically distant but strategically aligned middle powers are contributing to regional stability.

The focus then shifts to the digital and informational domain. **Jiro Minier** assesses the rapid evolution of Chinese cyberespionage capabilities and underscores the need for more adaptive and resilient responses. Complementing this analysis, **Sayaka Shingu and Diana Myers** argue that effective coordination and data-sharing among states with converging priorities is essential to countering China's expanding influence in emerging military technologies, including artificial intelligence.

The volume next turns to the challenge of Taiwan. **Eyck Freyman** makes the case for institutionalizing policy coordination among like-minded states to enhance coherence and credibility in approaches to cross-strait stability. Extending this discussion, **Michal Bokša** draws lessons from Ukraine to assess Taiwan's strategic thinking, identifying both enduring strengths and critical blind spots.

Beyond traditional security concerns, the essays also address economic and technological competition. **Blake Herzinger** explores how Southeast Asian countries are navigating intensifying pressures from economic fragmentation, supply chain realignment, and great-power rivalry. Looking to areas of untapped cooperation, **Chris Li** highlights biotechnology as a strategically significant yet underdeveloped domain in which deeper alignment could yield both security benefits and public goods.

Finally, the volume addresses the resilience of critical infrastructure. **Pratnashree Basu, Takuma Matsu, Momiji Natsuki, and Bich Tran** examine how enhanced maritime domain awareness can strengthen the protection of subsea cables—an often-overlooked but essential foundation of economic security and digital connectivity in the Indo-Pacific.

Euro-Atlantic Naval Cooperation in the Indo-Pacific: Strategic and Lasting?

By Agnieszka Kurzej

2021 marked the beginning of a new phase in Europe's commitment to and engagement in the Indo-Pacific. That year, a United Kingdom (UK) carrier strike group, led by one of the UK's two aircraft carriers, and joined by a Dutch frigate, a US destroyer (the USS Sullivans), and a squadron of US F-35s, sailed from the UK to Japan and back. This seven-month-long deployment was the first time the UK's new aircraft carrier, HMS Queen Elizabeth, sailed to the Indo-Pacific. The carrier strike group navigated over 50,000 nautical miles, making port calls for diplomatic and trade opportunities as well as conducting military exercises.[1] Building ties, whether military, diplomatic, or economic, while modeling "Global Britain" was a prime goal of the UK's banner deployment that year and was part of a wider "tilt" to the Indo-Pacific.[2]

Concurrent with this deployment, other European countries (including France, Germany, Italy, and others) were sending naval assets to the Indo-Pacific. France's Charles de Gaulle carrier strike group sailed to the Indian Ocean in 2021, where it exercised with Japan, Australia, and India.[3] The United States expressed support for these deployments, and in some instances participated through coordination or combined deployments and exercises.

But were these European deployments symbolic one-offs, or do they represent a continuing commitment to the Indo-Pacific? As Europe focuses on supporting Ukraine and ensuring its own security, will European navies still sail to the Indo-Pacific? Indeed, should European nations continue to spend attention and resources on two distant theaters?

Decades in the Making

At the time, the UK's deployment to the Indo-Pacific may have seemed like a one-off. In fact, it marked the culmination of ten years of US–UK carrier cooperation, underpinned by a Statement of Intent signed by US Secretary of Defense Leon Panetta and UK Secretary of State for Defence Phillip Hammond in 2012.[4] In April 2023, the US Department of Defense and UK Ministry of Defence renewed their cooperation for another decade, signing a second Statement of Intent, following their successful deployment in 2021.[5] Also in 2021, Navy heads from the United States, United Kingdom, and France signed a trilateral statement, committing to increasing their maritime cooperation globally.[6]

Meanwhile, European countries started to articulate how their interests are linked to and rooted in the Indo-Pacific, including ensuring global peace and prosperity, the security of trade routes, and the protection of the rules-based international order, in national-level strategy documents. France was the first European Union state to publish an Indo-Pacific strategy in 2019,[7] followed in 2020 by Germany[8] and the Netherlands.[9] In 2021, the European Union published its own strategy for cooperation in the Indo-Pacific.[10] Italy used its G7 presidency in 2024 to stress the interconnectedness between Euro-Atlantic and Indo-Pacific security.[11] These strategies acknowledge that "any significant crisis in one of these two theaters would have a direct political, economic and security impact on the other"[12] and serve as a foundation for continued European naval deployments to the Indo-Pacific.

European countries have continued to deploy their navies to the Indo-Pacific despite the drastic change in security dynamics on the European continent following Russia's full-scale invasion of Ukraine in February 2022. While Europe has increased defense spending and support to Ukraine, it has also continued to act globally. In 2024 alone, German Navy vessels transited the Taiwan Strait for the first time in two decades[13] and an Italian carrier strike group, led by the aircraft carrier Cavour, completed a five-month deployment to the region.[14] In fact, the war in Ukraine has demonstrated how the two theaters are intertwined by shining a light on the increased alignment between Russia and China. China's supply of critical components and minerals to Russia for its war effort has underscored the global nature of this war, and in some cases has mobilized European partners to take action not just in Europe but in the Indo-Pacific as well.[15]

In 2025, the UK and France have continued to deploy naval assets to the Indo-Pacific, building on the successes of previous ones. The UK deployed its second carrier, the HMS Prince of Wales, to the region on a scale similar to that of HMS Queen Elizabeth's deployment in 2021. Though France has a permanent miliary presence in the Indo-Pacific due to its territories there, 2025 was the first time in 57 years that a French carrier strike group sailed to the region.[16] French President Emmanuel Macron delivered this year's keynote speech at the Shangri-La Dialogue in Singapore, where he addressed the growing relationship between Europe and the Indo-Pacific, particularly as it relates to national security.[17] It is clear that European states have a vested interest in the region and are dedicating time and resources to building relationships there.

Continuing the Trend in 2025

All these developments suggest that European navies have built enduring ties in the region and will continue to sail to the Indo-Pacific despite an increasing focus on security dynamics in Europe. These deployments, often conducted in bilateral or "minilateral" formats, build interoperability and allow for training opportunities between regional and European partners in a multitude of multinational combinations. They are not meant to take European focus away from home or to bring NATO to the Indo-Pacific; rather, European military deployments to the Indo-Pacific underscore shared values and a commitment to upholding freedom of navigation and international law on a global scale.

Naval deployments can spur cooperation in other areas as well. In 2021, the Japanese Ambassador to the UK noted that the carrier strike group's deployment to Japan "symbolized the 'new level' of defense and security cooperation between Japan and the UK".[18] Indeed, "Euro-Pacific" cooperation has flourished in other areas as well; examples are the creation of AUKUS, a trilateral submarine and advanced technologies partnership among Australia, the United Kingdom, and the United States, and the Global Combat Air Program, under which the United Kingdom, Japan, and Italy are working together on a new fighter jet.[19] As Berti notes, "industrial cooperation could be an engine for fostering strategic convergence across theaters" and builds interoperability from the ground up.[20]

Conclusion

Looking ahead, if Europe's long-term goal is to increase its presence and engagement in the region, it will be important for European militaries to continue their cooperation with Indo-Pacific partners by continuing to exercise multilaterally, build interoperability, and gain regional expertise. It is too early to tell how developments in Ukraine will affect Europe's willingness and ability to deploy to the Indo-Pacific in the coming years, but it would take time to rebuild European navies' capability to deploy to the region if Europe were to slash engagement now.

On their end, Indo-Pacific states could clarify to partners in Europe their expectations for European engagement in the region. European deployments to and participation in combined military exercises in the Indo-Pacific are sometimes perceived as largely symbolic and lacking in strategic purpose and utility.[21] In fact, as made clear during conversations at the 2025 Young Strategists Forum, participants from across the Indo-Pacific region have so far appreciated Europe's presence in the region, saying that it shows Europe has a stake in Indo-Pacific security while exchanging expertise and building interoperability. For their part, European and American participants noted the importance of Japan's support to Ukraine, including its solidarity on sanctions against Russia and provision of training to Ukrainian forces.[22] From the US perspective, a global coalition in support of Ukraine sends a strong message to Russia—and other would-be aggressors—that unilateral power grabs matter to the whole world, not just one region, and will not go unanswered. To avoid misperceptions, Indo-Pacific partners could convey the benefits of cooperation to European counterparts more clearly both in government channels and to the public, including by coordinating messaging on the value of working together to tackle interconnected threats.

European naval deployments to the Indo-Pacific over the last few years have not only achieved their stated goals—forging ties, upholding the rules-based order, and exercising freedom of navigation, among others—it has also shown Europe is a credible military player in the region, with valid interests and capacity to act, albeit in a limited way. Building connective tissue between European and Indo-Pacific partners now will pay dividends if a contingency in the Indo-Pacific were to occur. Continued cooperation in the region now would improve communication, coordination, and capability to respond to a potential crisis in the future, if needed. Europe's first priority will of course always be its own security, but it has proven over the last few years it can indeed act globally in concert with Indo-Pacific partners.

Disclaimer:

The views and opinion expressed in this research are purely of the authors and do not represent any government, institute, or organization that they belong to.

Endnotes

[1] US Navy, "USS The Sullivans Completes Historic Deployment with HMS Queen Elizabeth and UK CSG 21, Marking the Culmination of Decade-Long Bilateral Effort", November 24, 2021. https://www.navy.mil/Press-Office/Press-Releases/display-pressreleases/Article/2857734/uss-the-sullivans-completes-historic-deployment-with-hms-queen-elizabeth-and-uk/

[2] Office of the Prime Minister, "Global Britain in a Competitive Age: Integrated Review of Security, Defence, Development, and Foreign Policy", March 2021. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/975077/Global_Britain_in_a_Competitive_Age-_the_Integrated_Review_of_Security__Defence__Development_and_Foreign_Policy.pdf

[3] Xavier Vavasseur, "French Carrier Strike Group Begins 2021 Deployment", U.S. Naval Institute, February 23, 2021. https://news.usni.org/2021/02/23/french-carrier-strike-group-begins-2021-deployment

[4] US Department of Defense and UK Ministry of Defence, "Statement of Intent Regarding Enhanced Cooperation on Carrier Operations and Maritime Power Projection", January 5, 2012. https://data.parliament.uk/DepositedPapers/Files/DEP2012-0189/DEP2012-0189.pdf

[5] US Department of Defense, "Readout of Secretary of Defense Lloyd J. Austin III's Bilateral Meeting With UK Secretary of State for Defence Ben Wallace", April 17, 2023. https://www.defense.gov/News/Releases/Release/Article/3365437/readout-of-secretary-of-defense-lloyd-j-austin-iiis-bilateral-meeting-with-uk-s/

[6] US Navy, "U.S., U.K., French Navies Reaffirm Commitment to Increased Cooperation", June 3, 2021. https://www.navy.mil/Press-Office/Press-Releases/display-pressreleases/Article/2643609/us-uk-french-navies-reaffirm-commitment-to-increased-cooperation/

[7] Céline Pajon, "France's Indo-Pacific Strategy", Institut Français des Relations Internationales, June 15, 2024. https://www.ifri.org/en/external-publications/frances-indo-pacific-strategy

[8] German Federal Foreign Office, "Germany – Europe – Asia: shaping the 21st century together": The German Government adopts policy guidelines on the Indo-Pacific region", January 9, 2020. https://www.auswaertiges-amt.de/en/aussenpolitik/regionaleschwerpunkte/asien/german-government-policy-guidelines-indo-pacific-2380510

[9] Full text of the Dutch government's Guidelines on the Indo-Pacific available here: Indo-Pacific: Guidelines for strengthening Dutch and EU cooperation with partners in Asia - "The World and Japan" Database, https://worldjpn.net/documents/texts/FOIP/20201100.O1E.html

[10] Joint Communication to the European Parliament and the Council, "The EU strategy for cooperation in the Indo-Pacific", September 16, 2021. https://www.eeas.europa.eu/sites/default/files/jointcommunication_2021_24_1_en.pdf

[11] Italian Prime Minister's Office, "Apulia G7 Leaders' Communiqué", June 15, 2024. https://www.g7italy.it/wp-content/uploads/Apulia-G7-Leaders-Communique.pdf

[12] Benedetta Berti, "Enhancing Euro-Atlantic and Indo-Pacific Theater Cooperation: What Is NATO's Role?", Sasakawa Peace Foundation, March 28, 2025. https://www.spf.org/iina/en/articles/benedetta_berti_01.html

[13] Alexander Ratz and Yimou Lee, "German navy makes rare transit of sensitive Taiwan Strait", Reuters, September 13, 2024. https://www.reuters.com/world/asia-pacific/german-navy-makes-rare-transit-sensitive-taiwan-strait-2024-09-13/

[14] Dzirhan Mahadzir, "Carrier Cavour's Pacific Deployment Extends Italy's Reach in the Pacific, Say Admiral", U.S. Naval Institute, October 11, 2024. https://news.usni.org/2024/10/11/carrier-cavours-pacific-deployment-extends-italys-reach-in-the-pacific-say-admiral

[15] Kyrylo Ovsyaniy, Anna Myroniuk, Schemes, and Carl Schreck, "China Supplying Key Chemicals For Russian Missiles, RFE/RL Investigation Finds", Radio Free Europe/Radio Liberty, January 30, 2025. https://www.rferl.org/a/china-critical-minerals-russia-weapons-ukraine-2024/33295674.html

[16] Martin Manaranche, "Insights on the French 'Clemenceau 25' Indo-Pacific Deployment", Naval News, July 19, 2025. https://www.navalnews.com/naval-news/2025/07/insights-on-the-french-clemenceau-25-indo-pacific-deployment/

[17] International Institute for Strategic Studies, "President of the French Republic Emmanuel Macron delivers the Keynote Address", May 30, 2025. https://www.iiss.org/events/shangri-la-dialogue/shangri-la-dialogue-2025/plenary-sessions/keynote-address/

[18] Ambassador Hajime Hayashi, "Ambassador's message on the return of the UK Carrier Strike Group (CSG21)", Japan's Embassy in the UK, December 9, 2021. https://www.uk.emb-japan.go.jp/itpr_en/211210amb.html

[19] BAE Systems, "Global Combat Air Programme", accessed February 23, 2025. https://www.baesystems.com/en/product/global-combat-air-programme

[20] Berti, "Enhancing Euro-Atlantic and Indo-Pacific Theater Cooperation".

[21] Max Bergmann, "Europe's Military Role in the Indo-Pacific: Play the Long Game", Internationale Politik Quarterly, September 26, 2024. https://ip-quarterly.com/en/europes-military-role-indo-pacific-play-long-game

[22] Prime Minister Fumio Kishida, "Investing in the Future: Japan's Unique Contribution to Ukraine", Government of Japan, February 19, 2024. https://www.japan.go.jp/kizuna/2024/03/japans_unique_contribution_to_ukraine.html

Signal, Deny, Punish: A Convergence of German, Australian, and Japanese Deterrence Strategies to Uphold a Free and Open Indo-Pacific

By Dr. Iain MacGillivray, Dr. Masatoshi Murakami, and Dr. Maximillian Ernst

Introduction

The Indo-Pacific region has become a crucial economic hub with 80 percent of worldwide trade passing through the region. In this important region, geopolitical tensions have intensified as regional powers enhance their military capabilities, and disputes have arisen around flashpoints like Taiwan and the South China Sea, straining relations between the People's Republic of China (PRC) and other nations. Despite these challenges, maintaining a free and open Indo-Pacific remains a shared goal for countries in the region. The idea of a "Free and Open Indo-Pacific" has been central to the defense strategies of key nations.[1] Numerous major countries have focused on deterring and countering negative behaviors in the Indo-Pacific. This foundational principle continues to be one of the pillars that nations in the region use to promote stability in this important but increasingly contested area.

This paper examines how three prominent nations—Germany, Australia, and Japan—positioned in three distinct regions of the globe execute their "Free and Open Indo-Pacific policies." It emphasises their use of military resources and deterrence strategies, considering their unique geographical contexts, priorities, and capabilities. The analysis argues that strategic concentric circles arise from differing priorities and geographical proximity, influencing the levels of strategy, deterrence, development, and deployment of each country's military capabilities. Despite these variations, a common goal emerges as all three nations strive to uphold a free and open Indo-Pacific.

Germany: A European Perspective on the Indo-Pacific

Germany has steadily increased its security engagement in the Indo-Pacific since the 2020 publication of its Indo-Pacific strategic guidelines.[2] The document lays out Germany's interests in the region—regional peace and stability, economic cooperation, and sustainable supply chains (among others)—and shows its ambition to work alongside regional value partners to achieve these objectives. This has been most visibly demonstrated through the deployment of the German Navy, Air Force, and Army to the region. Along with other important partners such as India, South Korea, and Singapore, Japan and Australia have been key anchor points in the German Armed Forces' deployments to the Indo-Pacific. During the 2021 Indo-Pacific Deployment (IPD21), the frigate Bayern sailed to the region, conducting joint exercises and naval diplomacy with like-minded partners. The port calls made by the Bayern included Perth and Darwin as well as Tokyo. In 2024, Germany further deepened its presence with the deployment of two Navy vessels, the supply ship Frankfurt am Main and the frigate Baden-

Wuerttemberg, as part of IPD24, once again including a port call in Tokyo.[3]

In 2022 and 2024, the German Air Force deployed transport, tanker, and fighter aircraft to Australia to participate in the air combat exercise Pitch Black and the naval combat exercise Kakadu. On the return flight to Europe, the German Air Force made stops in South Korea and Japan. In 2023, the German Army, along with Navy infantry and Air Force components, participated in the Talisman Sabre exercise in Australia.[4] Germany's increasing military presence in the Indo-Pacific aligns with the European Union's (EU) Indo-Pacific strategy.[5] The EU, as well as individual member states such as France and the Netherlands, have articulated Indo-Pacific strategies that emphasize open shipping lanes, multilateral cooperation, and a stable security environment. Germany's deployments complement these European efforts by contributing to military exercises, strengthening partnerships, and promoting regional stability. This signals Germany's commitment to a Free and Open Indo-Pacific and its willingness to impose diplomatic and economic costs on states that deteriorate regional stability by the unilateral use of military force or economic coercion against like-minded partners.

As a significant European economic power, Germany's security engagement lends additional credibility to the EU's broader geopolitical approach in the Indo-Pacific. The German Indo-Pacific strategy was published under the conservative and social democrat coalition government of Chancellor Angela Merkel (until 2021), and the consistent naval, air force, and army deployments of the past four years were executed under the coalition of Chancellor Olaf Scholz (2021–2025). This demonstrates that Germany's Indo-Pacific strategy and its commitment to the region enjoy a broad political consensus among all major parties of the political centre.[6] It is very likely that Germany, under a conservative and social democrat coalition from 2025 onwards, will continue its engagement in the Indo-Pacific, alongside regional partners such as Australia and Japan. By participating in joint exercises such as RIMPAC, Germany strengthens interoperability with Australia, Japan, and other like-minded partners, notably the United States, in reinforcing collective deterrence measures against China's increasingly revisionist posture.[7]

Germany's military presence in the Indo-Pacific, as well as broader European efforts, signal a commitment to deterring unilateral attempts to undermine regional stability. By working alongside partners such as Australia, Japan, and the EU, Germany reinforces a security framework that promotes cooperation, economic stability, and adherence to international law. This sustained engagement underscores Germany's evolution from a traditionally Eurocentric security posture to one that acknowledges the significance of the Indo-Pacific, underlining the interlinkages between the Indo-Pacific and Euro-Atlantic theatres.

Australia: Between a Rock and a Hard Place

Australia is a middle-power maritime nation reliant on shipping and significantly dependent on maintaining a free and open Indo-Pacific and the rules-based order. Its economy hinges on growth and trade with countries in the region, particularly its longstanding strong economic relations with the PRC.[8] In 2025, however, Australia finds itself caught between the need to maintain friendly relations with regional trading partners, specifically China, and its longstanding security alliance with the United States.

Australia's geographic position means that its defense strategy focuses on maintaining open and free maritime routes while safeguarding its northern areas

from adversarial presence. Australian policymakers have embraced a maritime strategy and a "strategy of denial" prioritising deterrence through military capabilities as a core principle of its national power (economic, diplomatic, military, cultural) to sustain a free and open Indo-Pacific.[9] This emphasis is reflected in the 2023 Defence Strategic Review (DSR) and the 2024 National Defence Strategy (NDS),[10] which identify "deterrence by denial" as the cornerstone of Australia's military strategy in the region.

Deterrence by denial aims to "degrade the adversary's likelihood of success or at least influence their estimate of it sufficiently to dissuade action".[11] Australia seeks to deter potential aggressors by developing capabilities that encourage them to reconsider military engagement.[12] The country's existing and developing alliance frameworks are crucial to these capabilities. For instance, Japan and Australia have strengthened their partnership and seek increased US commitments to the region and the Pacific. However, a decline in US global influence poses challenges for the strategic policies of both Australia and Japan.[13]

A key part of Australia's strategy for a free Indo-Pacific is modernising its military. This shift, detailed in the DSR and NDS, moves away from past expeditionary roles to focus on the immediate Indo-Pacific region. Consequently, Australia is evolving to a joint force emphasising naval and air power while also reshaping its land forces to concentrate on littoral operations.[14] Australia's defense forces continue to host and work with US Marines in the north of the country (as they have done since 2011) and, like Japan, has acquired land-based missile defenses for power projection and territorial protection. Overall, advancements in Australia's military capabilities and alliance integration signify constructive progress. This shift indicates Australia's awareness of its strategic vulnerabilities, especially in northern archipelagic areas and the Pacific.[15]

Australia's adaptation to the changing strategic environment, especially with the retrenchment of US power and decline of the rules-based order, is a key development in the new evolving order in the Indo-Pacific. Strengthened relationships and increased strategic integration with Japan and European allies like Germany, who are aiming for a more substantial presence in the region, can lay a solid foundation for enhancing defense posture in the Indo-Pacific, potentially securing maritime lines of communication and trade routes against bellicose behaviour.

Japan: At the Coalface of Indo-Pacific Tension

Japan is located in proximity to three nuclear-armed adversaries, namely China, Russia, and North Korea, and thus is geographically at the front line of the rivalry with what we might call the authoritarian triangle. These three countries have been stepping up collaboration since the Russian invasion of Ukraine. Japan is committed to upholding a free and open Indo-Pacific and is adopting three pillars of defense.

The first pillar involves strengthening its defense of the first island chain. Japan is increasing its military presence in Okinawa, its region closest to China, while considering potential contingencies in Taiwan and the Senkaku Islands. The Japanese government plans to double its defense budget by 2027, positioning itself as the third-largest military spender worldwide.[16] Japan plans to develop counterstrike capabilities that can reach an attacking country to counter a ballistic missile attack, while maintaining the country's longstanding framework of the Exclusively Defense-Oriented Policy. Such counterstrike capabilities serve as a deterrent by punishment, as they will inevitably punish an adversary who decides to invade Japanese territory.

As for the second pillar, Japan is deepening its military integration with the United States and launched the Joint Operations Command in March 2025. The Joint Operations Command will be responsible for Japan's Ground, Maritime, and Air Self-Defense Forces in peacetime and in the event of a conflict.

Striking developments are also emerging for the third pillar. Security collaboration with like-minded countries is a critical component of the December 2022 National Security Strategy (NSS).[17] The National Defense Strategy (NDS), a subordinate document to the NSS, lists, respectively, Australia, India, the UK, France, Germany, Italy, and NATO as like-minded partners.[18] Momentum towards broad security collaboration was pressed by Prime Minister Shinzo Abe, who is recognised as the father of the Quad framework.

Security cooperation with a like-minded country extends well beyond the personal connections of political leaders and is becoming increasingly institutionalised. Japan and Germany held Foreign and Defense Ministers' Meetings in April 2021 and November 2022.[19] These so-called 2+2 meetings serve as an important platform for bilateral security cooperation, allowing Japan to outline the strategic frameworks of both countries. The Acquisition and Cross-Servicing Agreement (ACSA) between the two nations was enacted in July 2024.[20] This was a milestone as a legally binding security agreement, distinct from the Defense Equipment and Technology Transfer Agreement signed in 2017. A training fleet of the Japan Maritime Self-Defense Forces made a port call in Hamburg in the summer of 2024.[21]

Australia is considered Japan's most significant security partner after the United States. The Japan-Australia Joint Declaration on Security Cooperation, signed by the prime ministers of both nations in 2022, serves as a fundamental document for the coming decade. Their ties are increasingly focused on military cooperation amid heightened tensions across the geopolitical landscape. Trilateral collaboration between Australia, Japan, and the US is also crucial. Australia and the US have welcomed Japanese participation in their force posture in northern Australia.[22]

Conclusion: Converging Strategic Circles of Deterrence

Germany, Australia, and Japan have a crucial stake in upholding a free and open Indo-Pacific. Their ongoing collaboration can significantly deter negative actions while strengthening trade and economic ties, to the benefit of both the region and the global community. A major conclusion of this paper is that the Indo-Pacific strategies of these nations can be represented as "strategic circles of deterrence," illustrated in Figure 1 below.

Germany is positioned in the outer circle, utilising a broad deterrence-by-signalling approach based on presence, values, capabilities, and communication. Despite the distance between Europe and the Indo-Pacific, Germany's engagement, along with that of the EU, is crucial, given deepening economic and military

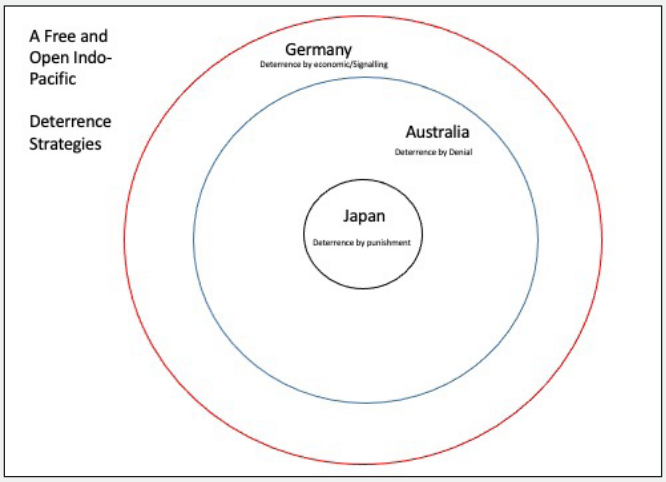

Figure 1: Circles of Deterrence

ties with the region. The second circle encompasses Australia, which, because of its maritime and trade interests in the Indo-Pacific, particularly with China, has adopted a deterrence-by-denial strategy to prevent adversarial behaviour in the region, which may challenge its interests and stability. Australia holds a stake in the region but enjoys flexibility in its strategy. At the core, Japan stands out in its deterrence-by-punishment due to its proximity to China, North Korea, and Russia. Japan has developed integrated alliance networks, accentuating its capability to counter any threats to its interests.

It is essential to recognise that the Indo-Pacific and Euro-Atlantic theatres are gradually converging. These strategic concentric circles are essential for grasping each country's views on the Indo-Pacific and its method for facing challenges, deterring negative actions, and enhancing collaboration to support key connections. Effective implementation of these defense strategies could lead to a collective effort to ensure regional stability and reap benefits, even with a gradual US withdrawal. If these initiatives deepen over time, it may be feasible to maintain and strengthen a robust, free Indo-Pacific.

Endnotes

[1] *Shinzo Abe, "Confluence of the Two Seas", Ministry of Foreign Affairs, August 22, 2007. https://www.mofa.go.jp/region/asia-paci/pmv0708/speech-2.html*

[2] *Federal Government of Germany, "Policy Guidelines for the Indo-Pacific: Germany–Europe–Asia Shaping the 21st Century Together", Federal Foreign Office, August 2020. https://www.auswaertiges-amt.de/resource/blob/2380514/f9784f7e3b3fa1bd7c5446d274a4169e/200901-indo-pazifik-leitlinien--1--data.pdf*

[3] *Alex Luck, "German Navy Wraps Indopacific Deployment - A Naval News Assessment", Naval News, December 10, 2024. https://www.navalnews.com/naval-news/2024/12/german-navy-wraps-indopacific-deployment-a-naval-news-assessment/*

[4] *Peter Müller, "Talisman Sabre 23", Bundeswehr. https://www.bundeswehr.de/en/organization/army/talisman-sabre-23*

[5] *European External Action Service, "EU Strategy for Cooperation in the Indo-Pacific", April 19, 2021. https://eeas.europa.eu/headquarters/headquarters-homepage/96741/eu-strategy-cooperation-indo-pacific_en*

[6] *Maximilian Ernst, "De-Risking: How Germany's Indo-Pacific Deployments Support Berlin's Economic Strategy Towards China" [CSDS Policy Brief], Centre for Security, Diplomacy and Strategy, February 6, 2024. https://csds.vub.be/publication/de-risking-how-germanys-indo-pacific-deployments-support-berlins-economic-strategy-towards-china/*

[7] *Bundesministerium der Verteidigung, "Verteidigungsminister Pistorius Besucht Die Indo-Pazifik-Region", 2023. https://www.bmvg.de/de/themen/dossiers/engagement-im-indopazifik/minister-besucht-strategisch-bedeutsame-indo-pazifik-region*

[8] *James Laurenceson and Michael Zhou, "Small grey rhinos: Understanding Australia's economic dependence on China", Australia-China Relations Institute, UTS, May 22, 2019. https://www.uts.edu.au/acri/research-and-opinion/reports/small-grey-rhinos-understanding-australias-economic-dependence-china*

[9] *Jennifer Parker, "An Australian maritime strategy: Resourcing the Royal Australian Navy", Australian Strategic Policy Institute, October 2023. https://www.aspi.org.au/report/australian-maritime-strategy*

[10] *Australian Department of Defence, "National defence: Defence Strategic Review 2023", 2023. https://www.defence.gov.au/about/reviews-inquiries/defence-strategic-review; Australian Department of Defence, "National Defence Strategy", 2024. https://www.defence.gov.au/about/strategic-planning/2024-national-defence-strategy-2024-integrated-investment-program*

[11] *Chris Rahman and Prakash Gopal, "The Role of Deterrence in Australian Strategic Thought: Implications for ANZUS", Journal of Indo-Pacific Affairs 7, no. 6., Sept.-Oct. 2024, 84–100, p. 87.*

[12] *Iain MacGillivray, "Military Denial: the basis of deterrence, and of response if deterrence fails", The Strategist, ASPI, April 24, 2024. https://www.aspistrategist.org.au/military-denial-the-basis-of-deterrence-and-of-response-if-deterrence-fails/*

[13] *Sam Roggeveen, "Donald Trump and the Relative Decline of US Power in Asia", Internationale Politik Quarterly, May 6, 2024. https://ip-quarterly.com/en/donald-trump-and-relative-decline-us-power-asia*

[14] *Iain MacGillivray, "To 'protect-and-project' – A call for Australian land power in the Indo-Pacific", The Interpreter, Lowy Institute, February 27, 2025. https://www.lowyinstitute.org/the-interpreter/protect-project-call-australian-land-power-indo-pacific*

[15] *Chris Smith, "The implications of emerging changes in land warfare for the focused all-domain defence force", Australian Strategic Policy Institute, December 13, 2024. https://www.aspi.org.au/report/implications-emerging-changes-land-warfare-focused-all-domain-defence-force*

[16] *Mirna Galic, "How Fumio Kishida Shaped Japan's Foreign Policy", United States Institute of Peace, August 22, 2024. https://www.usip.org/publications/2024/08/how-fumio-kishida-shaped-japans-foreign-policy*

[17] *"National Security Strategy of Japan", December 2022. https://www.cas.go.jp/jp/siryou/221216anzenhoshou/nss-e.pdf*

[18] *国家防衛戦略(National Defense Strategy of Japan), December 2022, pp. 15-16. https://www.cas.go.jp/jp/siryou/221216anzenhoshou/boueisenryaki.pdf*

[19] *Ministry of Foreign Affairs of Japan, "Japan-Germany Foreign and Defense Ministers' Meeting ("2+2")," April 2021. https://www.mofa.go.jp/press/release/press4e_002994.html*

Ministry of Foreign Affairs of Japan, "Japan-Germany Foreign and Defense Ministers' Meeting," November 2022. https://www.mofa.go.jp/erp/c_see/de/page4e_001299.html

[20] *Ministry of Foreign Affairs of Japan, "Entry into Force of the Agreement between the Government of Japan And the Government of the Federal Republic of Germany Concerning Reciprocal Provision of Supplies and Services Between the Self-Defense Forces of Japan and the Armed Forces of the Federal Republic of Germany," July 2024. https://www.mofa.go.jp/press/release/pressite_000001_00427.html*

[21] *Consulate-General of Japan in Hamburg, "Besuch der japanischen Ausbildungsflotte im Hamburger Hafen," September 2024. https://www.hamburg.emb-japan.go.jp/itpr_ja/11_000001_01279.html*

[22] *US Department of Defense, "Australia-Japan-United States Trilateral Defense Ministers' Meeting November 2024 Joint Statement", November 16, 2024. https://www.defense.gov/News/Releases/Release/Article/3967118/australia-japan-united-states-trilateral-defense-ministers-meeting-november-202/*

Evolving to Meet the Chinese Cyberespionage Revolution

Indo-Pacific Partnership as an Essential Pillar of Proactive Cyber Defense

By Jiro Minier

In comments to the press in June 2025, the newly promoted head of the FBI's Cyber Division, Brett Leatherman, described a "long game by [China] to map our infrastructure, to steal our data, to erode our strategic edge from the inside out".[1]

He is far from a lone voice in this dire assessment of the Chinese cyberespionage challenge. Following a closed-door briefing for US senators held in late 2024 concerning the sweeping compromise of multiple telecommunications operators by Chinese cyberespionage actor Salt Typhoon, Senator Richard Blumenthal went so far as to state that the "extent and depth and breadth of Chinese hacking is absolutely mind-boggling— that we would permit as much as has happened in just the last year is terrifying".[2]

Remarkably, the language used to characterize this challenge was similarly stark a decade ago. In 2012, NSA Director Keith Alexander described US intellectual property theft via cyberespionage as "the greatest transfer of wealth in history".[3] In the ensuing years, however, the threat has continued to evolve seemingly uninhibited by various efforts to manage it, with the maturation of Chinese cyberspace capabilities accompanied by a steady tempo of high-impact espionage campaigns.

Far from being a threat confined to the United States, Chinese cyberespionage has also wreaked havoc among its closest allies in the Indo-Pacific. Perhaps most spectacularly, recent media reports claim that the Japanese government was warned in 2020 by US counterparts that Chinese cyberespionage activity had compromised sensitive Japanese classified defense networks[4] and diplomatic telecommunications systems.[5]

Such activity has continued unabated since, with the Japanese National Police Agency warning in early 2025 of a half-decade-long China-linked cyberespionage effort targeting Japanese entities including high-tech firms, think tanks, and policymakers.[6]

In South Korea, meanwhile, the National Intelligence Service highlighted the significant proportion of China-linked "cyber security incidents of high significance" impacting the country in 2024.[7] Commentators have highlighted South Korea's relative exposure to Chinese cyberespionage efforts, with a recent Chosun Ilbo editorial stating that "South Korea is wide open to China's cyber infiltration" and detailing challenges such as the exclusive focus of national counterespionage legislation on North Korean threats.[8]

Recent policy discussions, particularly in the United States, have focused disproportionately on the important, linked, but different issue of Chinese cyber-enabled critical infrastructure prepositioning.[9] It is essential that policymakers understand the Chinese cyberespionage threat as a distinct, maturing, and pervasive challenge with specific characteristics and more insidious long-term impacts on Indo-Pacific partners' geostrategic potential and capabilities.[10]

Even as Indo-Pacific partners such as the United States, Japan, and South Korea shift towards active cyber defense policies and postures to contend with the Chinese cyberespionage threat, it is essential to understand that this alone is insufficient in the face of such a threat, and that this shift demands equally active cyber defense and partnership enhancements. Strongly enhanced cooperation between partners to deconflict activity, define targeting opportunities, and deny malicious actors easy wins are essential elements in minimizing the possible confusion caused by active cyber defense capabilities while maximizing their meaningful impact.

Understanding the (Advanced Persistent) Threat

For decades, cyberespionage activity linked back to China has been leveraged in the suspected pursuit of a diverse range of objectives: the deep penetration of targets and industries of long-term espionage interest, the active support of geostrategic and geoeconomic objectives, the monitoring of diaspora, minority, and dissident activity, and more.[11] Crucially, however, the last half-decade has seen considerable shifts both in the capabilities enabling such activity as well as in the maturation of the ecosystem underpinning it.

In more recent years, China has led the field in the domain of zero-day exploitation publicly attributed to a known state activity nexus, in which attackers are able to compromise targets via the use of a vulnerability unknown even to the vendors of the product being exploited (as opposed to the much less challenging exploitation of publicly known product vulnerabilities). For example, in an assessment of zero-day exploitation observed in 2024, Google researchers noted that "PRC threat groups remained the most consistent government-backed espionage developer and user of zero-days," with nearly 30% of "traditional espionage" activity in this category attributed to China-linked threat actors.[12]

This steady pipeline of zero-day exploits appears to be just one aspect of an increasing ability on the part of China-linked threat actors to bring a highly specialized knowledge of the products that they are exploiting to bear on targets. Certain recent campaigns have involved activity in target networks that evince an extraordinary depth of understanding of targeted products, making use of undocumented product features in their attack chains.[13] At times, China-linked threat actors have been able to leverage such specialist knowledge on the fly, bypassing fixes for vulnerabilities and tools used to detect malicious activity created and deployed as part of the defensive effort against their malicious activity in real time.[14] This specialization is far from constrained to products, as evinced by the focus of certain threat actors on entire industry verticals and their specialist technology (such as the aforementioned targeting of telecommunications sector targets worldwide by Chinese cyberespionage actor Salt Typhoon).[15] The command and control of these operations is facilitated by complex proxy infrastructure (so-called "operational relay box networks") built up via the compromise of insecure appliances worldwide and used to conceal and obfuscate the origins of malicious activity.[16]

Far from being tied to a single identifiable actor, these developments are underpinned by a complex facilitatory ecosystem of agencies, contractors, and service providers.[17] This is actively reinforced by the Chinese regulatory and legislative agenda, with cybersecurity talent within China effectively weaponized[18] via mechanisms such as hacking competitions, mandatory vulnerability reporting legislation, and the subordination of vulnerability reporting processes to intelligence interests.[19]

Partnership in Proactive Times

In the face of this rapidly maturing threat, recent years have seen a corresponding global shift towards the pursuit of more proactive cybersecurity policies.[20] States are increasingly formulating cybersecurity policy options that are varyingly framed as active, proactive, persistent, and more, blurring the lines between traditional paradigms of cyberspace offense and defense. In the United States, where Biden administration cybersecurity policies focused more heavily on shoring up security weaknesses at home,[21] recent statements by Trump administration officials reflect a desire to "have all the tools necessary to go on offense"[22] and to be able to "respond in kind"[23] in cyberspace.

This is also prominently visible in the Indo-Pacific region. In Japan, the last half decade has seen an even sharper shift, with tentative first steps towards mild responsive measures to cyberattacks in 2021, such as public attribution (wherein malicious activity is formally attributed to a given state or government of origin),[24] overshadowed only several years later by the adoption of legislation on a fully-fledged "Active Cyber Defense" posture permitting actions including the neutralisation of adversary command and control infrastructure.[25] In South Korea, the 2024 National Cybersecurity Strategy goes so far as to explicitly call for an offensive posture to buttress the country's cybersecurity situation,[26] an evident shift from the 2019 Strategy's language on "active countermeasures."[27]

However, far from addressing this evolving threat, the unilateral pursuit of active cyber defense options by multiple states in parallel is liable to generate more confusion and adverse effects than meaningful impacts; a coherent active defense posture against the Chinese cyberespionage threat will demand enhanced partnership between Indo-Pacific partners on difficult topics. Three key areas in which such partnership must be in evidence include deconfliction, target definition, and denial of exploitation opportunities.

First, the existence of multiple parallel active cyber defense efforts raises obvious deconfliction challenges between partners. For example, one partner's actions to disrupt threats in cyberspace may have inadvertent effects on another state's essential visibility over malicious activity. Partners must therefore ensure that active cyber defense measures are accompanied by an enhanced deconfliction posture that addresses potential friction between their respective interests and security demands, understanding that one partner's solution may be another partner's problem. This could include elements such as established pipelines by which states can raise operational objections to active cyber defense actions proposed by partners where prior notification is feasible, or strategic working groups established between regional security partners to take stock on a regular basis of the outcomes of active cyber defense actions and to assess both positive and adverse effects resulting from them.

Secondly, partners must collectively define targeting opportunities, sharing information and insights on the Chinese cyberespionage threat to ensure that active cyber defense measures are tailored to the idiosyncrasies of China's multifaceted cyberespionage support apparatus. The effectiveness of approaches tailored to target ecosystems is in evidence elsewhere in the cyber policy debate. For example, UK officials have stated that the multinational law enforcement operation targeting ransomware syndicate LockBit in 2024 pursued the fragmentation of the affiliate model underpinning the operation.[28] In the same way, a cooperative approach to building up a picture of the Chinese cyberespionage ecosystem may allow partners to disrupt key nodes and dependencies in this ecosystem with an eye to lasting, long-term impact.

Finally, partners must coordinate to deny Chinese cyberespionage actors access to the insecure appliances and vulnerable software that have been their hunting grounds of choice in recent years. Proactivity does not simply entail cyberspace entanglements with malicious actors. In contending with the widespread abuse of small-office/home-office (SOHO) routers or internet of things (IoT) devices by Chinese threat actors to constitute anonymisation infrastructure,[29] for example, enhanced multinational rulemaking surrounding end-of-life devices in these categories, such as the incentivisation of their replacement by users, could serve as an equally effective means by which to deny this terrain to malicious actors.

Taken together, the implications are clear. In the face of a rapidly evolving and professionalising Chinese cyberespionage threat, the attractiveness of a more active cyber defense posture from a political and policy standpoint in many countries is clear. However, far from allowing these countries to pivot fully and unilaterally to the offense, an active cyber defense posture that is deconflicted, targeted, and comprehensive enough to meaningfully contend with this threat will demand far greater coordination and cooperation between regional partners than ever before.

Endnotes

[1] *Martin Matishak, "FBI cyber leader: US can't forget about China's 'Typhoon' groups amid Mideast conflict", The Record, June 24, 2025. https://therecord.media/china-typhoon-groups-espionage-fbi-cyber-brett-leatherman*

[2] *David Shepardson and Richard Cowan, "US senators vow action after briefing on Chinese Salt Typhoon telecom hacking", Reuters, December 4, 2025. https://www.reuters.com/world/us/us-agencies-brief-senators-chinese-salt-typhoon-telecom-hacking-2024-12-04/*

[3] *Emil Protalinski, "NSA: Cybercrime is 'the greatest transfer of wealth in history'," ZDNET, July 10, 2012, https://www.zdnet.com/article/nsa-cybercrime-is-the-greatest-transfer-of-wealth-in-history/*

[4] *Ellen Nakashima, "China hacked Japan's sensitive defense networks, officials say", The Washington Post, August 8, 2023. https://www.washingtonpost.com/national-security/2023/08/07/china-japan-hack-pentagon/*

[5] *The Yomiuri Shimbun, "U.S. Warned Japan of China's Hacking of Official Diplomatic Telegram System; Reinforcing Cybersecurity Key Concern", February 5, 2024. https://japannews.yomiuri.co.jp/politics/defense-security/20240205-166966/*

[6] *National Policy Agency, "MirrorFace によるサイバー攻撃について（注意喚起）" [Regarding the cyber attack by MirrorFace], January 8, 2025. https://www.npa.go.jp/bureau/cyber/pdf/20250108_caution.pdf*

[7] *Kim Arin, "Seoul's spy agency accuses China of major cyber attacks", The Korea Herald, January 24, 2024. https://www.koreaherald.com/article/3312349*

[8] *The Chosun Daily, "Editorial: South Korea is wide open to China's cyber infiltration", May 21, 2025. https://www.chosun.com/english/opinion-en/2025/05/21/AM52IWKADVFVVAYCEA7TM5I4JU/*

[9] *Ryan Lucas, "Wray warns Chinese hackers are aiming to 'wreak havoc' on U.S. critical infrastructure", NPR, January 31, 2024. https://www.npr.org/2024/01/31/1228153857/wray-chinese-hackers-national-security*

[10] *Erica Lonergan and Michael Poznansky, "A Tale of Two Typhoons: Properly Diagnosing Chinese Cyber Threats", War on the Rocks, February 25, 2025. https://warontherocks.com/2025/02/a-tale-of-two-typhoons-properly-diagnosing-chinese-cyber-threats/*

[11] *Nathan Thornburgh, "The Invasion of the Chinese Cyberspies", Time, August 29, 2005. https://time.com/archive/6674509/the-invasion-of-the-chinese-cyberspies/*

[12] *Casey Charrier et al, "Hello 0-Days, My Old Friend: A 2024 Zero-Day Exploitation Analysis," Google Cloud (blog), April 29, 2025. https://cloud.google.com/blog/topics/threat-intelligence/2024-zero-day-trends*

[13] *Scott Henderson, Cristiana Kittner, Sarah Hawley, and Mark Lechtik, "Suspected Chinese Threat Actors Exploiting FortiOS Vulnerability (CVE-2022-42475)", Mandiant (blog), January 19, 2023. https://cloud.google.com/blog/topics/threat-intelligence/chinese-actors-exploit-fortios-flaw*

[14] Matt Lin, Robert Wallace, Austin Larsen, Ryan Gandrud, Jacob Thompson, Ashley Pearson, and Ashley Frazer "Cutting Edge, Part 3: Investigating Ivanti Connect Secure VPN Exploitation and Persistence Attempts", Mandiant (blog), February 27, 2024. https://cloud.google.com/blog/topics/threat-intelligence/investigating-ivanti-exploitation-persistence

[15] Insikt Group, "RedMike (Salt Typhoon) Exploits Vulnerable Cisco Devices of Global Telecommunications Providers", Recorded Future, February 13, 2025. https://www.recordedfuture.com/research/redmike-salt-typhoon-exploits-vulnerable-devices

[16] Michael Raggi, "IOC Extinction? China-Nexus Cyber Espionage Actors Use ORB Networks to Raise Cost on Defenders," Mandiant (blog), May 22, 2024. https://cloud.google.com/blog/topics/threat-intelligence/china-nexus-espionage-orb-networks

[17] Coline Chavane and TDR Team, "A three-beat waltz: The ecosystem behind Chinese state-sponsored cyber threats", Sekoia, November 2024. https://blog.sekoia.io/wp-content/uploads/2024/11/A-three-beat-waltz-The-ecosystem-behind-Chinese-state-sponsored-cyber-threats.pdf

[18] Eugenio Benincasa, "From Vegas to Chengdu: Hacking Contests, Bug Bounties, and China's Offensive Cyber Ecosystem", CSS ETH Zurich, June 10, 2024. https://css.ethz.ch/en/center/CSS-news/2024/06/from-vegas-to-chengdu-hacking-contests-bug-bounties-and-chinas-offensive-cyber-ecosystem.html

[19] Priscilla Moriuchi & Bill Ladd, "China's Ministry of State Security Likely Influences National Network Vulnerability Publications", Recorded Future, November 16, 2017. https://www.recordedfuture.com/blog/chinese-mss-vulnerability-influence

[20] Richard J. Harknett, "America's allies are shifting: Cyberspace is about persistence, not deterrence", CyberScoop, October 2, 2024. https://cyberscoop.com/cybersecurity-deterrence-persistence-richard-harknett-dod-strategy/

[21] Sean Lyngaas, "Biden makes last big move to protect US networks from hackers from China and elsewhere", CNN, January 16, 2025. https://edition.cnn.com/2025/01/16/politics/biden-cybersecurity-executive-order

[22] Martin Matishak, "NSC official: Trump administration will 'change the script' on offensive side", The Record, May 2, 2025. https://therecord.media/trump-administration-change-the-script-on-offensive-hacking

[23] Tim Starks, "CIA nominee tells Senate he, too, wants to go on cyber offense", CyberScoop, January 15, 2025. https://cyberscoop.com/cia-nominee-john-ratcliffe-cyber-offense/

[24] "サイバー攻撃 名指し「反撃」" [Cyber attacks: naming and fighting back], Nikkei, May 13, 2021. https://www.nikkei.com/article/DGKKZO71808330S1A510C2CM0000/

[25] "「能動的サイバー防御」導入の法律 参院本会議で可決.成立" [The law to introduce "active cyber defense" was passed and enacted at the plenary session of the House of Councillors], NHK, May 16, 2025. https://www3.nhk.or.jp/news/html/20250516/k10014807531000.html

[26] Natasha Wood, "South Korea's 2024 Cyber Strategy: A Primer", Center for Strategic & International Studies, August 2, 2024. https://www.csis.org/blogs/strategic-technologies-blog/south-koreas-2024-cyber-strategy-primer

[27] National Security Office, "National Cybersecurity Strategy", June 20, 2019. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/National%20Cybersecurity%20Strategy_South%20Korea.pdf

[28] Akshaya Asokan, "Operation Cronos Is Disrupting LockBit, Says UK Official", Bank Info Security, October 10, 2024. https://www.bankinfosecurity.com/operation-cronos-disrupting-lockbit-says-uk-official-a-26508

[29] Department of Justice, "U.S. Government Disrupts Botnet People's Republic of China Used to Conceal Hacking of Critical Infrastructure", January 31, 2024. https://www.justice.gov/archives/opa/pr/us-government-disrupts-botnet-peoples-republic-china-used-conceal-hacking-critical

Shared Data, Shared Peace: An East Asian & ASEAN Vision

Strengthening Indo-Pacific cooperation to ensure the responsible development and use of AI in defense: a case for South Korea, Japan, and ASEAN

By CAPT Diana Y. Myers & Dr. Sayaka Shingu

Introduction

Artificial intelligence (AI) is the new geopolitical front line in the strategic competition between the United States and the People's Republic of China (PRC). For both countries, however, the choice (true dichotomy or not) between regulation and safety versus innovation and prosperity is shaping global alliances. The accelerating global race towards achieving Artificial General Intelligence (AGI) has underscored the critical need to maintain a competitive edge in AI while ensuring its ethical, responsible, and equitable development.

AI's potential for weaponization in defense necessitates proactive policymaking to establish a collaborative environment among like-minded nations. This approach will facilitate the sharing, collaboration, and development of AI capabilities that can bolster the national defense of regional partners and uphold international norms, especially in a digital-rich environment, like the Indo-Pacific.

In the Indo-Pacific, the landscape of AI competition is particularly salient for the Association of Southeast Asian Nations (ASEAN). The PRC has been notably proactive, engaging in numerous AI partnerships and research collaborations with these nations. This trend highlights the urgent need for alternative, robust AI collaboration frameworks that can effectively compete with and counterbalance the PRC's growing influence, particularly leveraging the comparative advantages that South Korea and Japan hold in this sector.

AI cooperation between the PRC and ASEAN nations spans various levels of government in Beijing. We see high-level initiatives like the PRC–Malaysia AI collaboration between the China Academy of Information & Communications (who reports directly to the Ministry of Industry and Information Technology) and the University of Malaysia. Local governments, such as those of Jiangsu, Sichuan, and Guangxi provinces in the PRC, are working with countries like Singapore to develop industrial technology parks. These parks aim to import AI technology and attract AI-related investments through vehicles like the China-ASEAN Technology Transfer Center and Collaborative Innovation (CATTC). Headquartered in Nanning, Guangxi, the CATTC is a public institution formally established by the Chinese Ministry of Science and Technology and ASEAN member states where its primary purpose is to enhance the transfer of advanced and applicable technologies between the PRC and ASEAN, facilitating joint research, technology, training, and personnel exchanges.[1] The PRC's strategic partnerships with ASEAN nations are further strengthened by the expansion of Chinese tech giants like Tencent and Huawei in Southeast Asia. These companies provide essential Internet-of-Things (IOT) technologies, making the PRC an attractive

AI collaboration partner. This deepening reliance on Chinese technology should persuade competing nations to enhance their AI collaboration efforts and offer viable alternatives.

AI in Defense

As AI's utility expands across various sectors, its integration into defense strategies has become increasingly vital. PRC's defense doctrine, which emphasizes mechanization (机械化), informatization (信息化), and intelligentization (智能化) as key phases of military modernization, highlights this trend. In its military modernization efforts, the PRC is pursuing intelligentization, which is the integration of advanced AI and autonomous systems into its armed forces. This transformation from a data-networked force to an AI-driven, cognitive force aims to gain a decisive advantage in what the People's Liberation Army (PLA) refers to as the "cognitive space," potentially offering significant asymmetric advantages on the battlefield. AI-driven battlespace management systems in the future, for instance, can enable commanders to make faster, more informed decisions by synthesizing vast amounts of information more rapidly than an adversary without such a system. This capability will likely be a crucial force multiplier, particularly for nations with limited conventional military resources. AI-driven defense applications, including automatic target recognition, autonomous drones, and sensor-to-shooter systems, enhance the efficiency and precision of military operations. These technologies improve battlespace awareness and enable more accurate targeting of high-value targets, minimizing waste and maximizing effectiveness.

Existing Regulatory AI Frameworks for Defense Use

More countries are becoming interested in discussing the use of AI in the military domain. In July 2022, the United States, the United Kingdom, and France submitted to the UN's Nonproliferation Treaty Review Conference a working paper emphasizing the importance of maintaining human control and involvement in all actions critical to informing and implementing sovereign decisions concerning nuclear weapons employment.[2] On November 15, 2023, U.S. President Joe Biden and Chinese President Xi Jinping "affirmed the need to address the risks of advanced AI systems and improve AI safety through U.S.-China government talks".[3] On the general concept of AI use in the military domain, the September 2024 summit of Responsible AI in the Military Domain (REAIM) hosted in Seoul, produced the Blueprint for REAIM Action, which confirmed the significance of maintaining human control.[4]

Following the summit, South Korea, the Netherlands, and other like-minded countries submitted a UN resolution titled "Artificial intelligence in the military domain and its implications for international peace and security".[5] This is the United Nations' first initiative in adopting a resolution on the military use of AI, and the UN Secretary General is expected to issue a comprehensive report in 2025 to seek the views of Member States and observer States on the opportunities and challenges posed to international peace and security by the application of artificial intelligence in the military domain.

Leaders of AI in Northeast Asia: Japan and South Korea

To effectively counter the PRC's growing influence over the commercial and defense applications of AI, it is imperative for nations with aligned AI development goals to collaborate, innovate, and leverage their combined capabilities, resources, and markets. Japan and South Korea, as leaders in AI software and hardware in the region, are well-positioned to spearhead this effort through joint ventures and strategic alliances. As a means of trilateral cooperation, the United States could collaborate with Japan and South Korea to create a means for AI defense collaboration.

Japan

The Cabinet Office of Japan issued an updated "AI Strategy" in 2022,[6] aiming to contribute to the Sustainable Development Goals based on the three principles of "dignity for humanity," "diversity," and "sustainability." A concept paper on AI policy issued by the Cabinet Office of Japan in 2024 underlined the importance of involving multi-stakeholders for considering future regulations and of using private expertise when it comes to regulatory implementation.[7]

Following the G7 Summit in Hiroshima in May 2023, the G7 leaders launched the Hiroshima AI Process, whose objective is to discuss the rapid development and spread of generative AI.[8] Building upon this initiative, the "Hiroshima AI Process Comprehensive Policy Framework" was compiled at the ministerial-level meeting in December 2023 as "the first international policy framework consisting of guidelines and a code of conduct with the aim of promoting the spread of safe, secure, and reliable advanced AI systems". The Hiroshima AI Process has since expanded to include various actors beyond the G7, including developing countries and emerging economies.

Japan's Ministry of Defense also formulated two documents in 2024: the "Basic Policy for Promoting the Use of AI in the Ministry of Defense" and the "Comprehensive Strategy for Cyber Human Resources in the Ministry of Defense." These documents' purpose is to serve as "a compass for promoting the use of AI and securing and developing cyber human resources".[9]

South Korea

The Ministry of Science and ICT (MSIT) has released the "Blueprint for Korea's AI Innovation to Achieve AI G3 Status," outlining a vision for public-private collaboration across four national AI projects. These projects include establishing the "National AI Computing Center," securing private sector investments in AI development, achieving high AI adoption rates in industry and the public sector, and establishing leadership in AI governance and safety.[10] This policy discusses the building of regional AI innovation hubs and deploying various AI capabilities in national defense through "the development of military security policies and expansion of defense AI infrastructure", promoting responsible use of AI in the military context and across security sectors.

Additionally, the Ministry of National Defense under President Yoon Suk Yeol's administration announced its "Defense Reform 4.0" in 2024, identifying the securing of AI-based core advanced combat platforms as one of its five core pillars, in addition to investing in robust defense AI foundation in its overall research and development investments.[11]

Policy Recommendation

To effectively compete with the PRC's AI proliferation in the Indo-Pacific, it is crucial to offer ASEAN nations and other regional partners a compelling alternative. This alternative should provide a cost-effective, robust, and superior AI architecture that facilitates military modernization for better battlespace awareness that adheres to responsible global AI regulatory norms for defense-use. A federated data network presents a viable solution, enabling the secure sharing and analysis of defense data across multiple countries, feeding into a robust model that populates a common operating picture (COP) for decision makers to use.[12] A federated architecture could integrate structured, unstructured, and semi-structured inputs from multinational sensor systems, generating a unified dataset to support the development and training of advanced AI models for use in defense. An initiative spearheaded by regional AI leaders like South Korea and Japan, with US backing, could offer a more appealing proposition for ASEAN countries hesitant to align solely with the United States over the PRC.

Federated Data Network for Enhanced Defense Capabilities

A federated data network led by South Korea and Japan, comprising interconnected data lakes across different nations, would offer a powerful architecture for managing and analyzing diverse defense-related data. Participating countries would contribute by sharing sensor-collected data from their respective platforms, allowing the model to be trained on more robust data. The data within this network can be used to train AI models for a range of defense applications. For instance, large language models (LLMs) can be developed to enhance strategic decision-making. Additionally, models for automatic target recognition can be trained using imagery data from regional sensors of participating nations, improving surveillance and reconnaissance for like-minded allies and partners for a collaborative and seamless COP.

To ensure seamless access to and utilization of these capabilities, a robust cross-domain solution can be implemented by South Korea and Japan. Such a solution would facilitate the integration of AI-derived insights into each country's command and control (C2) platforms. Alternatively, a standardized digital C2 platform could be designed to provide a COP for all participating nations, enhancing battlespace awareness and coordination, a platform akin to the U.S. Department of Defense's efforts to develop the Joint All-Domain Command and Control (JADC2).[13]

Participation in this advanced AI capability framework necessitates adherence to stringent cybersecurity protocols to protect the integrity and confidentiality of the data. Member countries must also comply with data standardization protocols outlined in the network's bylaws. These bylaws will include specific restrictions to safeguard sensitive information and ensure responsible use of the technology. For example, participating nations would be required to join a multilateral alliance led by South Korea and Japan that will prohibit the adoption of alternative AI solutions from competitors like the PRC and Russia. The partnership should also allow for data lake "dams" as required to control data flow into the system—this will allow countries the added flexibility to choose which partners they decide to share certain information with. Additionally, the use of this technology for domestic surveillance must be strictly prohibited.

The expansion of the data network and the inclusion of additional partner nations will necessitate the development of more data centers. These data centers would represent significant economic investment opportunities for ASEAN countries and priority would be given to participating nations. Investments in data center infrastructure should be contingent

upon meeting environmental sustainability criteria to minimize ecological impact.[14]

Conclusion

To effectively counter the PRC's expanding influence in the commercial and military domains of AI, States with convergent development priorities must coordinate their efforts. This requires fostering innovation and integrating their technological strengths, resources, and markets. Within the Indo-Pacific, Japan and South Korea are uniquely positioned to lead this effort, given their comparative advantages in AI software and hardware. These nations can assume a leading role through strategic partnerships and joint initiatives, providing a compelling alternative to regional partners, particularly ASEAN nations.

Our policy proposes an effective, robust, and superior multinational AI defense architecture that facilitates military modernization as a compelling alternative to the PRC. A federated data network provides a practical approach, allowing for the secure exchange and joint analysis of defense information among allied nations in the region. This inclusive framework would not only empower partners to participate more effectively in regional security initiatives but also ensure they benefit from advanced AI capabilities.

Similarly, the United States should engage with Tokyo and Seoul to institutionalize a trilateral framework for defense-focused AI collaboration for the region which can expand to include other regional partners like ASEAN. This framework would not only mitigate the PRC's proliferation of AI but also promote the ethical development and deployment of the technology by establishing shared guidelines and best practices. Ultimately, this collaborative effort will strengthen regional security and contribute to the global discourse on the responsible use of AI in the defense sector.

Disclaimer:

The views and opinion expressed in this research are purely of the authors and do not represent any government, institute, or organization that they belong to.

Endnotes

[1] *Ministry of Science and Technology of the People's Republic of China. n.d. "The 10th Forum on China-ASEAN Technology Transfer and Collaborative Innovation Opens in Nanning, Guangx", Accessed September 14, 2025. https://en.most.gov.cn/pressroom/202210/t20221009_182833.html*

[2] *2020 Review Conference of the Parties to the Treaty on the Non-Proliferation of Nuclear Weapons, "Principles and responsible practices for Nuclear Weapon States" (Working Paper), United Nations Office for Disarmament Affairs, July 29, 2024. https://documents.un.org/doc/undoc/gen/n22/446/53/pdf/n2244653.pdf*

[3] *White House, "Readout of President Joe Biden's Meeting with President Xi Jinping of the People's Republic of China", November 15, 2023. https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2023/11/15/readout-of-president-joe-bidens-meeting-with-president-xi-jinping-of-the-peoples-republic-of-china-2/*

[4] *Responsible AI in the Military Domain, "REAIM Blueprint for Action", September 2024. https://www.mofa.go.kr/www/brd/m_4080/down.do?brd_id=235&seq=375378&data_tp=A&file_seq=9*

[5] *United Nations, "Fourteen New Drafts, Including on Implications of Artificial Intelligence in Military Domain, Approved in First Committee by 34 Votes", November 6, 2024. https://press.un.org/en/2024/gadis3757.doc.htm; United Nations General Assembly, 79th Session, First Committee, "Agenda Item 98: General and complete disarmament" (UNdoc A/C.1/79/L.43), October 16, 2024. https://docs.un.org/en/A/C.1/79/L.43*

[6] *Cabinet Office of Japan, "AI Strategy 2022", April 22, 2022. https://www8.cao.go.jp/cstp/ai/aistratagy2022en.pdf*

[7] *Cabinet Office of Japan, "AI制度に関する考え方について" [A way of thinking regarding AI system], June 2024. https://www8.cao.go.jp/cstp/ai/ai_senryaku/9kai/shiryo2-1.pdf*

[8] *Hiroshima AI Process, 総務省「広島AIプロセス」." [A way of thinking regarding AI system], June 2024. https://www.soumu.go.jp/hiroshimaaiprocess/index.html*

[9] 防衛省「防衛省ＡＩ活用推進基本方針と防衛省サイバー人材総合戦略の策定について」令和６年７月２日 *https://www.mod.go.jp/j/press/news/2024/07/02a.html*

[10] *Ministry of Science and ICT, "MSIT Presents Blueprint for Korea's AI Innovation to Achieve AI G3 Status," September 26, 2024. https://www.msit.go.kr/eng/bbs/viewdo?sCode=eng&mId=4&mPid=2&pageIndex=&bbsSeqNo=42&nttSeqNo=1040&searchOpt=ALL&searchTxt=.*

[11] *Ministry of National Defense, "국가전략정보포털" [Defense Innovation 4.0], National Strategic Information Portal, February 28, 2023. https://nsp.nanet.go.kr/plan/main/detail.do?nationalPlanControlNo=PLAN0000035393.*

[12] *Technical considerations for building alliance-based COP have been previously explored in the NATO space context. See North Atlantic Treaty Organization Science & Technology Task Group, "Technical Considerations for Enabling a NATO-Centric Space Domain Common Operating Picture (COP)", December 2020. https://www.sto.nato.int/publications/STO%20Technical%20Reports/Forms/Technical%20Report%20Document%20Set/docsethomepage.aspx?ID=4480&FolderCTID=0x0120D5200078F9E87043356C409A0D30823AFA16F6010066D541ED10A62C40B2AB0FEBE9841A61&List=92d5819c-e6ec-4241-aa4e-57bf918681b-1&RootFolder=%2Fpublications%2FSTO%20Technical%20Reports%2FSTO%2DTR%2DSCI%2D279*

[13] *David Vergun, "DoD Officials Discuss Advancements in Joint All-Domain Command, Control", DOD News, February 28, 2022. https://www.defense.gov/News/News-Stories/Article/Article/2948282/dod-officials-discuss-advancements-in-joint-all-domain-command-control/*

[14] *Beth Stackpole, "AI Has High Data Center Energy Costs—but There Are Solutions", Ideas Made to Matter, MIT Sloan, January 7 2025. https://mitsloan.mit.edu/ideas-made-to-matter/ai-has-high-data-center-energy-costs-there-are-solutions*

Institutionalizing a Core Coalition for Taiwan Policy Alignment

By Dr. Eyck Freymann

The People's Republic of China's (PRC's) threat to Taiwan poses the most serious test of U.S. alliances in the Indo-Pacific. While military deterrence is critical, political deterrence through a strong, institutionalized coalition of allies is equally necessary. Unlike NATO's collective defense structure, the U.S.-led Indo-Pacific alliance system is fragmented, with no formal mechanism that it can use to coordinate responses to a crisis affecting Taiwan. The PRC appears increasingly inclined to exert economic and military pressure on Taiwan. Ad hoc diplomacy is no longer sufficient. The United States must move beyond informal consultations and institutionalize a core coalition of allies—which I will suggest should include Japan, Australia, Canada, and the United Kingdom—to ensure maximum policy alignment on Taiwan. This coalition must be structured to strengthen deterrence and coordinate crisis responses in a way that protects Taiwan while maintaining stability in the region.

One of the greatest challenges in preparing for a Taiwan contingency is the absence of institutionalized legal and political frameworks for responding to crises short of war. A full-scale invasion is only one among several possible scenarios. More likely are "gray-zone" contingencies, in which China seeks to alter the status quo through incremental coercion while avoiding an overt act of war. A selective blockade, or what Beijing might frame as a "quarantine" of Taiwan, is among the most probable scenarios. In such an event, China could use its maritime forces to interdict commercial and military shipments, declaring that it is enforcing customs regulations or anti-smuggling operations while stopping short of a formal act of war. Such a maneuver would test not only U.S. resolve but also the willingness of allies to challenge China's claims. Without prior legal and political coordination, allied responses are likely to be slow, hesitant, and inconsistent. In such a crisis, the lack of clear commitments from key U.S. allies could embolden Beijing to press further, gambling that political paralysis will allow it to shift the status quo in its favor without direct military confrontation.

Beyond the challenge of military coordination, any Indo-Pacific contingency—whether a blockade, missile crisis, or outright conflict—would immediately create massive disruptions to global supply chains. China has already demonstrated a willingness to use its dominance in key industries, such as rare earth processing, semiconductor manufacturing, and shipping logistics, to exert economic pressure on foreign governments and private companies. In a Taiwan crisis, Beijing would likely pressure multinational corporations to withdraw from Taiwan and cut off investment, while simultaneously coercing smaller states into denying basing rights or overflight permissions for U.S. and allied military operations. This dynamic drives the need for the United States and its partners to establish pre-crisis agreements on economic coordination. Without a coherent approach, individual companies and states will come under intense pressure to comply with PRC demands, thereby weakening deterrence. A core coalition should align on policies to counter China's economic coercion, including coordinated export controls, financial penalties for companies that submit to PRC pressure, and measures to secure alternative supply chains for essential goods.

The existing Indo-Pacific security architecture is not suited to meet these challenges. Unlike NATO, which provides a formal alliance framework with clear legal commitments, the U.S. Indo-Pacific alliance network is built from bilateral agreements, creating a fragmented structure that lacks mechanisms for coordinated crisis response. While NATO itself is unlikely to be extended into the Indo-Pacific, the institutional barriers to doing so illuminate the broader structural constraints facing Taiwan policy alignment. NATO operates on the principle of collective defense under Article V, but applying such a framework to Taiwan would require a fundamental shift in the security postures of key allies, particularly Japan, which has historically avoided explicit military commitments outside its constitutional self-defense framework. European states such as France have already resisted deeper NATO involvement in the Indo-Pacific, fearing that doing so would overextend European security commitments and provoke unnecessary confrontation with China.[1] These challenges suggest that instead of seeking a NATO-style expansion, the United States should focus on creating a separate but complementary structure: an Indo-Pacific coalition specifically designed to manage Taiwan-related crises and provide an agreed-upon mechanism for collective decision-making and response. The core of such a coalition should consist of four key U.S. allies: Japan, Australia, Canada, and the United Kingdom.

Japan is the most crucial actor given its geographic proximity and strategic interests. Tokyo has already signaled that a Taiwan contingency would directly affect Japanese security. In 2021, Deputy Prime Minister Taro Aso was quoted as saying at a private event that a Taiwan crisis could pose an existential threat to Japan, though he walked back the remarks when the story broke.[2] However, Japan has yet to adopt a legal framework that would enable decisive action in a crisis.[3]

Talk of a Japanese version of the Taiwan Relations Act (TRA) has circulated for decades among scholars and lawmakers, but it has never moved beyond vague calls for action.[4] (The U.S. version of the TRA notes that a PRC effort to change the status quo by force would constitute a matter of "grave concern" to the United States.) Several obstacles have prevented Japan from formally specifying its interest in Taiwan. These include: concerns about violating the 1972 Japan–China communiqué, the tricky politics of keeping Japan's governmental coalition(s) together; the pressure put on the government by the Japanese business lobby, Keidanren; continuing sensitivity around Article 9, the Japanese constitutional ban on warmaking; lack of consensus on what a "JTRA" would actually entail; and fear of PRC retaliation. These hurdles are real—but they are not insurmountable.

Rather than replicating the U.S. TRA wholesale, Japan should consider a phased, carefully structured approach. First, it could pass a basic law on Japan–Taiwan exchanges, explicitly reaffirming the "One China" language of 1972 while codifying nonmilitary areas of cooperation such as humanitarian relief, civil defense training, supply-chain security, and information sharing. This would provide a legal roof over existing practice without appearing to shift Tokyo's official position. Second, Japan could adopt a Diet resolution declaring cross-Strait stability a "vital interest" for Japan's security, thereby framing any Taiwan-related action as consistent with constitutional interpretations of collective self-defense. Third, to avoid economic blowback, Tokyo could pair any Taiwan legislation with broader economic security initiatives, including incentives for reshoring critical industries.

In the long term, a Japanese TRA would clarify Japan's commitments and establish a structured, flexible approach to Taiwan security, similar to the U.S. framework. Another part of U.S. policy toward Taiwan, which Japan, Australia, and the United Kingdom may

consider replicating, is the Six Assurances. These pledges, made bilaterally to Taiwan without the involvement of the PRC, represent a promise that the United States will not trade away Taiwan to the PRC or pressure it to negotiate unification under duress. Formalizing these sorts of commitments would help deter China by strengthening the credibility of collective deterrence.

Australia, as a rapidly strengthening U.S. security partner, is the next most significant player. Through the Australia-UK-U.S. pact (AUKUS), Australia has demonstrated a willingness to take on a greater role in Indo-Pacific security, but its legal commitments with respect to Taiwan remain undefined.[5] Given the growing Australian debate over its role in a Taiwan conflict, Canberra should similarly consider adopting a Taiwan Relations Act–style legal framework that defines its strategic posture in a Taiwan crisis. Doing so would help reinforce deterrence and clarify Australia's position in advance, reducing Beijing's ability to pressure Canberra into a neutral stance in a crisis.

The United Kingdom and Canada, while geographically distant, bring economic and diplomatic strength to any Indo-Pacific security structure. Both are already integrated into the Five Eyes intelligence network (along with Australian, New Zealand, and the United States) and maintain strong defense ties with the United States. The UK's increasing engagement in the Indo-Pacific, including naval deployments to the region, signals a growing commitment to regional stability. However, neither the UK nor Canada has a clear legal or political framework for addressing Taiwan, leaving their positions ambiguous. As part of a core coalition, these countries should align their policies with the United States and Japan by adopting formal declarations or legal frameworks that clarify their commitments.

Institutionalizing this coalition requires more than informal diplomatic dialogue. The United States should establish a Taiwan Security Coordination Council, modeled on NATO's North Atlantic Council, to provide a standing forum for allied coordination on Taiwan policy. This body should meet regularly at the ministerial level, with participation from defense, foreign affairs, and economic officials, to ensure ongoing policy alignment. In addition, an annual Indo-Pacific Leaders' Summit, taking place before the G7, should be established to reinforce high-level commitments and public messaging. These mechanisms would serve as both deterrent signals to China and practical coordination platforms for crisis scenarios.

Economic deterrence must also be built into this coalition. The coalition should develop pre-agreed financial and trade measures, including coordinated sanctions and asset freezes, to be enacted automatically in response to PRC aggression against Taiwan. Ensuring supply chain resilience should be another focus. China's ability to weaponize economic dependencies in a crisis means that the coalition must invest in alternative supply chains for critical products like rare earths, semiconductors, and active pharmaceutical ingredients.

Finally, this coalition must serve as a bridge between existing Indo-Pacific security structures and European partners who may be reluctant to engage in Taiwan-specific planning. Allied governments should explore mechanisms for issue-specific cooperation between NATO and Indo-Pacific security partners, particularly in areas such as military technology development, cyber defense, and intelligence sharing. Although France has resisted NATO's expansion into the region, the United States and its closest allies can still foster greater European involvement in discrete security initiatives that contribute to Taiwan's security without requiring full NATO integration.

The U.S. cannot afford to rely on strategic ambiguity and informal consultations alone to deter PRC

aggression against Taiwan. As Beijing actively seeks to exploit allied divisions and economic vulnerabilities, Washington must institutionalize a core coalition to ensure maximum policy alignment. By formalizing military, economic, and diplomatic coordination, this coalition can strengthen deterrence, provide a clear decision-making framework for crisis response, and prevent China from using legal and political ambiguity to its advantage. The failure to institutionalize allied coordination now risks paralysis in a future crisis. The time to act is before a Taiwan contingency forces a rushed and reactive response under immense political and economic pressure.

Endnotes

[1] *Stuart Lau and Laura Kayali, "Macron Blocks NATO Outpost in Japan Amid PRC Complaints", Politico, July 7, 2023. https://www.politico.eu/article/emmanuel-macron-block-nato-outpost-japan-china-complaints/*

[2] *Jesse Johnson, "Deputy PM says Japan must defend Taiwan with U.S.", The Japan Times, July 6, 2021. https://www.japantimes.co.jp/news/2021/07/06/national/taro-aso-taiwan-defense/*

[3] *Ministry of Foreign Affairs, Japan, "Joint Communique of the Government of Japan and the Government of the People's Republic of China", September 29, 1972. https://www.mofa.go.jp/region/asia-paci/china/joint72.html; Julian Ryall, "Aso Walks Back Claim Japan Would Join U.S. in Defence of Taiwan if Mainland PRC Forces Invade", South China Morning Post, July 6, 2021. https://www.scmp.com/week-asia/politics/article/3139995/aso-walks-back-claim-japan-would-join-us-defence-taiwan-if; Adam P. Liff, "Has Japan's Policy Toward the Taiwan Strait Changed?", Brookings Institution, August 23, 2021. https://www.brookings.edu/articles/has-japans-policy-toward-the-taiwan-strait-changed/*

[4] *Adam P. Liff, A "Taiwan Relations Act" for Japan?," Wilson Center, February 25, 2021. https://www.wilsoncenter.org/blog-post/taiwan-relations-act-japan*

[5] *Sang Hun Seok, "Expanding AUKUS Pillar 2: An Inclusive Indo-Pacific Alliance Structure", Royal United Services Institute, July 16, 2024. https://www.rusi.org/explore-our-research/publications/commentary/expanding-aukus-pillar-2-inclusive-indo-pacific-alliance-structure*

Taiwan's Strategic Thinking and Strategic Blind Spots: Lessons from Ukraine

By Michal Bokša

The Global Cooperation and Training Framework (GCTF)—a platform which specializes in using Taiwan's expertise for addressing global issues—has recently concluded its latest International Workshop on the Whole-of-Society Resilience Building, Preparation, and Response.[1] Although some of the questions are hard to confront, such as those related to Taoyuan Airport's contingencies in case tens of thousands of people flock to its perimeters for evacuation, the fact that they are being raised underscores the volatile security environment of the Indo-Pacific in general and the Taiwan Strait in particular. Today, Taiwan is not in a good spot. The People's Republic of China (PRC)'s gray zone activities around the island have become more frequent, Xi Jinping's directive for the People's Liberation Army (PLA) to be ready to invade Taiwan by 2027 continues to haunt local political elites,[2] and the determination of Taiwan's key partners to support it in case of a military escalation is increasingly uncertain.[3]

Despite a deteriorating security environment, Taiwan's long-term determination that no military measures will alter the relations of the two sides of the Taiwan Strait is both inspiring and commendable. Many recent policy and military decisions reinforce this determination. The extension of compulsory national service from four months to one year, a gradual increase in military spending, efforts to increase the retention of servicemembers through higher salaries, and expansion of strategic stockpiles are but a few of these measures and policy decisions.[4] Combined with civilian-led initiatives and organizations such as Kuma Academy, which strives to cultivate self-defense capability via a provision of a variety of trainings to a general public (70% of alumni are women, otherwise excluded from the compulsory national service),[5] the determination and resilience of the little island appears to be considerable.

In recent months, it has been hard not to notice that among Taiwan's political circles certain aspects of military strategic thinking seem to be either overlooked or, when asked during various Q&A sessions, left unanswered. These gaps become even more obvious when viewed through the lens of Ukraine's experience following Russia's full-scale invasion in February 2022. While drawing too many parallels between the war in Ukraine and a potential conflict in the Taiwan Strait can be misleading at best—and a fool's errand at worst—it would be equally unwise to ignore the critical lessons Ukraine's defense offers for Taiwan's military preparedness and strategic planning.

First, when the prospect of a Chinese military invasion of Taiwan arises in debates and discussions, high-ranking Taiwanese officials frequently emphasize that such an operation would take the PLA weeks to prepare. Their implication is clear: A 'strategic surprise' military action by Beijing is unlikely, given the logistical buildup such an operation would require. In theory, they are not wrong. A large-scale amphibious assault on Taiwan would be an immense undertaking, with estimates of the PLA troops required ranging between 400,000 and over two million.[6] However, the flaw in this assumption becomes evident when considering Ukraine's experience. Despite facing an analogous situation—with more than 175,000 Russian troops massed along its borders—Kyiv was caught off guard

when the invasion began in 2022.[7] Ukraine was not alone in its miscalculation; just days before the attack, many Western and international analysts remained skeptical that Russia would launch a full-scale war.[8]

Ukraine's experience—particularly the sequence of events that led to its strategic surprise in 2022—offers a scenario that could, to some extent, be replicated in the Taiwan Strait. More importantly, the likelihood of a similar trajectory unfolding within the next decade is relatively high, regardless of whether it ultimately culminates in a full-scale invasion of Taiwan. The reason so many were caught off guard by Russia's attack was the normalization of large-scale military drills. Over time, their frequency led to complacency, which, in turn, enabled the strategic surprise of 2022. If the PRC were to adopt a similar pattern—regularly massing troops under the guise of routine exercises—Taiwan and its allies would have to recognize this as a critical indication that Beijing might be moving closer to actualizing an invasion. After all, in February 2022, Vladimir Putin continued to insist that Russia's military maneuvers around Ukraine were "purely defensive" and "not a threat".[9] Taiwan must carefully consider how to respond should a comparable pattern begin to emerge.

Second, when Taiwanese representatives discuss the island's security vis-à-vis the PRC, they tend to overemphasize Taiwan's ability to repel an initial wave of attacks while skimming past the next steps, which demand far more attention but offer far fewer clear answers. Taiwan's military preparedness, commitment to its defense, and expanding stockpiles of critical supplies all indicate that the PLA could in the opening phase of an invasion face significant challenges. The Chinese military might struggle to establish air superiority, coordinate a large-scale joint operation, or successfully transport enough troops ashore.[10] After all, the second major strategic surprise of Russia's war in Ukraine was the astonishing failure of Russia's initial offensive to achieve its objectives. This failure culminated in one of the most striking tactical blunders of the war—the infamous 56-km-long convoy of armored vehicles, consisting of 10 Russian battalion tactical groups, immobilized for weeks due to shortages of food, fuel, ammunition, and effective communication.[11] The PLA could face a similar fate in the early stages of a Taiwan conflict, an envisaged outcome that, in itself, serves as a powerful deterrent for Chinese leadership.

Nevertheless, beyond repelling the PLA's initial assault, how would Taiwan fare if the PRC, like Russia in Ukraine, committed to a prolonged conflict while enforcing a military blockade of the island? How would Taiwan's partners, particularly the United States, respond? Strategic ambiguity regarding potential military support leaves room for speculation. However, lessons from Ukraine suggest that even if war breaks out and Taiwan initially stands alone (an outcome far from certain), the PRC's ability to deter Taiwan's partners from providing military aid or becoming involved in the conflict will weaken over time. When Russia first invaded Ukraine, Western democracies were largely hesitant to supply direct military assistance. But as Russia's initial deterrence faded, Western military aid—including armored vehicles, tanks, aircraft, and, most recently, long-range cruise missiles like Storm Shadow and ATACMS—grew dramatically.[12] There is little doubt that the PRC's ability to deter Western support or involvement in a Taiwan conflict would also erode, potentially even more quickly in the wake of the Ukraine war.

Time will undoubtedly work against Taiwan, as its stockpiles of essential military supplies, food, and energy deplete with the pace of the conflict. However, it will also work against the PRC. The longer Taiwan endures a protracted war, the greater the likelihood and intensity of Western support or involvement. Beijing would be wise to incorporate this trajectory into its own strategic calculations when assessing

the potential outcomes of any military action against Taiwan.

Lastly, understanding the Russia–Ukraine conflict from Beijing's perspective is crucial—especially since the PRC has almost certainly drawn its own lessons from the war, some of which could have significant implications for the PLA's future planning and operations. In particular, Russia's initial battlefield failures have likely reinforced doubts about the PLA's ability to successfully execute an invasion of Taiwan.[13] Given the immense political and military stakes involved, it is difficult to imagine China's leadership taking such a risk without first seeking to test and enhance the PLA's reliability, as well as gain operational experience—preferably in a lower-stakes environment.

Until now, China has largely been a risk-averse actor outside the Indo-Pacific. However, if this pattern shifts in the coming years—if Beijing becomes more willing to expose its military to conflict situations or assumes a greater role as a security provider—it would likely signal a serious effort to improve the PLA's readiness for high-stakes confrontations. In this context, regions such as eastern Afghanistan or Myanmar could offer opportunities for the PLA to expand its security role without significantly jeopardizing China's political and diplomatic standing. While not all operational experience gained in these areas would be directly applicable to a potential amphibious invasion of Taiwan, such engagements could still help the PLA to address critical shortcomings—particularly in areas where Russia failed early in its 2022 invasion of Ukraine, such as poor military planning, logistical challenges, and low combat readiness.[14]

In conclusion, for the potential escalation in the Taiwan Strait, the war in Ukraine can serve as simultaneously a warning and a source of insight. It can demonstrate that strategic surprises are still possible, even with tens of thousands of troops deployed alongside a country's border, but it can also reveal how an invader's ability to deter outside involvement can weaken over the course of a prolonged war. As of now, Taiwan's security mainly hinges on strengthening its own deterrence. The capacities to repel an initial assault and to sustain itself in a drawn-out war are the two critical factors Taiwan should prioritize. Importantly, Beijing's greatest fear is not merely a failed invasion but a protracted war that draws in Western support, turning a swift military operation into a costly quagmire. For Taiwan, the worst-case scenario is undeniably represented by the PRC's full-scale invasion. Ultimately, the best deterrence Taiwan has is its ability to convince Beijing that the little island has the capacity to transform Taiwan's worst-case scenario into the PRC's worst-case scenario.

Endnotes

[1] Global Cooperation and Training Framework, "Strengthening Whole-of-Society Resilience", March 7, 2025. https://www.gctf.tw/en/news_detail110_0.htm; American Institute in Taiwan, "GCTF Workshop Strengthens International Collaboration on Whole-of-Society Resilience", March 4, 2025. https://www.ait.org.tw/gctf-workshop-strengthens-international-collaboration-on-whole-of-society-resilience/

[2] The Economist, "China's stunning new campaign to turn the world against Taiwan", February 9, 2025. https://www.economist.com/international/2025/02/09/chinas-stunning-new-campaign-to-turn-the-world-against-taiwan

[3] Alexander Panetta, "The day the old American order cracked in the Oval Office", CBC News, February 28, 2025. https://www.cbc.ca/news/world/american-order-zelenskyy-trump-1.7472000.

[4] AP, "Taiwan says boost in defense spending coming amid China threats", March 4, 2025. https://apnews.com/article/china-taiwan-defense-spending-bcdd4fa977cbccccf6d480b03870b59b

[5] Kuma Academy, "About Kuma Academy", 2024. https://kuma-academy.org/about?lang=en

[6] Alex Gatopoulos, "How difficult would it be for China to invade Taiwan?", Al Jazeera, April 4, 2022. https://www.aljazeera.com/features/2022/4/4/how-difficult-would-it-be-for-china-to-invade-taiwan

[7] Mike Eckel, "How Did Everybody Get The Ukraine Invasion Predictions So Wrong?", Radio Free Europe/ Radio Liberty, February 17, 2023. https://www.rferl.org/a/russia-ukraine-invasion-predictions-wrong-intelligence/32275740.html

[8] Harun Yilmaz, "No, Russia will not invade Ukraine", Al Jazeera, 09 February 2022. https://www.aljazeera.com/opinions/2022/2/9/no-russia-will-not-invade-ukraine; Jonas J. Driedger and Mikhail Polianski, "Utility-based predictions of military escalation: Why experts forecasted Russia would not invade Ukraine", Contemporary Security Policy, Vol. 44, no. 4, 544–560. https://doi.org/10.1080/13523260.2023.2259153

[9] Alix Culbertson, "Ukraine crisis: Putin says military drills 'purely defensive' and 'not a threat' as Western leaders warn invasion imminent", Sky News, February 18, 2022. https://news.sky.com/story/ukraine-crisis-putin-says-military-drills-purely-defensive-and-not-a-threat-as-western-leaders-warn-invasion-imminent-12545284

[10] Lonnie Henley, "Many Ways to Fail: The Costs to China of an Unsuccessful Taiwan Invasion", United States Institute of Peace, November 5, 2024. https://www.usip.org/publications/2024/11/many-ways-fail-costs-china-unsuccessful-taiwan-invasion

[11] Claire Press and Svitlana Libet, "How Russia's 35-mile armored convoy ended in failure", BBC, February 22, 2023. https://www.bbc.com/news/world-europe-64664944

[12] Murray Brewster, "First ten armoured vehicles promised to Ukraine to be delivered by summer, Blair says", CBC, April 26, 2024. https://www.cbc.ca/news/politics/ukraine-russia-armoured-vehicles-blair-1.7186785; Lauren Kent, Allegra Goodwin, and Oren Liebermann, "Ukraine fires British-French Storm Shadow missiles into Russia for first time, say reports", CNN, November 21, 2024. https://edition.cnn.com/2024/11/20/europe/ukraine-uk-storm-shadow-missiles-russia-intl-latam/index.html; Thomas d'Istria, Chloé Hoorman, Philippe Ricard, and Faustine Vincent, "US allowing Ukraine to use ATACMS missiles in Russia is unlikely to change balance of power", Le Monde, November 19 , 2024. https://www.lemonde.fr/en/international/article/2024/11/19/us-allowing-ukraine-to-use-atacms-missiles-in-russia-is-unlikely-to-change-balance-of-power_6733314_4.html

[13] Hope Yen, "CIA chief: China has some doubt on ability to invade Taiwan", AP, February 26, 2023. https://apnews.com/article/russia-ukraine-taiwan-politics-united-states-government-eaf869eb617c6c356b2708607ed15759

[14] Seth G. Jones, "Russia's Ill-Fated Invasion of Ukraine: Lessons in Modern Warfare", Center for Strategic and International Studies, June 1, 2022. https://www.csis.org/analysis/russias-ill-fated-invasion-ukraine-lessons-modern-warfare

The Growing Divide: Southeast Asia's Struggle for Balance in a Fragmenting Global Economy

By LCDR Blake Herzinger

The intensifying economic and technological decoupling between the United States and China is redrawing the map of global trade, technology, and finance. Nowhere is this more keenly felt than in Southeast Asia. In a region that has long embraced strategic autonomy while profiting from deep engagement with both superpowers, neutrality is becoming harder to sustain. For decades, member states of the Association of Southeast Asian Nations (ASEAN) balanced their relationships deftly, trading freely with China while engaging in security cooperation and investment with the United States. While regional actors argue that they should not have to choose between Washington and Beijing, the growing divide between the two largest economies is making such choices unavoidable in key sectors such as technology, advanced research, biotech, investment, and national security.

The Historical Roots of Decoupling

It is tempting to trace the current fragmentation to COVID-19, or to the Trump administration's first wave of tariffs. But the rupture began earlier, with China's own efforts to reduce dependence on foreign technology.[1] As early as 2003, the Chinese Communist Party began laying the groundwork for its Medium-to-Long Term Plan for Science and Technology Development, implemented in 2006, which aimed to cut foreign tech reliance in half by 2020. This 15-year roadmap established benchmarks for China to become an "innovation-oriented society" by 2020 and a world leader in science and technology by 2050. That effort intensified under the 2015 "Made in China 2025" program, which set aggressive goals for domestic self-sufficiency in ten strategic industries (information technology, robotics and AI, aerospace, shipping, railways, energy, materials, medical equipment and medicines, agriculture, and power equipment).[2] Subsequent government directives accelerated efforts to crowd out foreign firms by limiting foreign hardware and software in state institutions.[3]

Beijing's intention was clear: to cultivate national champions, secure supply chains, and compete directly with leading global technology firms. The United States took time to recognize the trend and began recalibrating its posture during President Obama's second term, initially through export controls and later through full-scale industrial policies aimed at reshoring production and securing its own tech ecosystem. The Biden administration's subsequent push to "de-risk" has since evolved into the Trump administration's more disruptive "Liberation Day" tariffs, injecting fresh volatility into Southeast Asia's external economic environment.

Ranging from ships to chips, US tariffs have upended more than trade relations as many countries now grapple with new levels of uncertainty about the future of their relationships with the United States. As new tariff announcements emanate from Washington on a near-weekly basis, Southeast Asian economies in "Factory Asia" are actively seeking détente with the Trump administration but also driving forward with new

free-trade agreements with partners like the EU and Gulf Cooperation Council. While many policymakers and pundits[4] in the United States seem convinced that globalization is over, Asia is unpersuaded. And data appears to back Asia's view—global trade volume continues to rise while the US share of that trade decreases. In fact, as US trade as a percentage of GDP continues to fall, the difference in trade openness between the US and the rest of the world has widened to 34 percent, the largest gap in the last 50 years (see Figure 1).

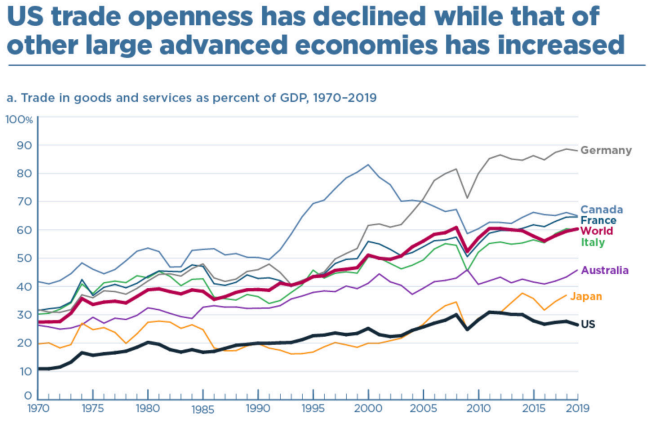

Figure 1: Trade openness, US vs. other major economies
Source: *Peterson Institute for International Economics, April 19, 2021*

Implications for Southeast Asia

From telecommunications and payments to biotech research and military procurement, competing spheres of influence are taking shape, and Southeast Asia's role as a linchpin in global supply chains makes it particularly vulnerable to these significant shifts. In telecommunications, the United States and its allies are promoting alternatives to Chinese tech infrastructure—such as Open Radio Access Network (Open RAN) for 5G, which is designed to open up mobile network architecture and allow providers to include non-proprietary subcomponents from multiple vendors—and providing an alternative to exclusive communications systems relationships with China that Washington and its allies view as problematic. China continues to champion its own standards and systems, with an eye on carrying its commanding lead in 5G technology into the 6G environment. For Southeast Asian countries, adoption of one architecture over another signals alignment and carries implications for trade, investment, and security cooperation.

In advanced research and biotechnology, new US laws demonstrate increasing suspicion of Chinese partnerships, threatening to fracture collaborative networks that Southeast Asia relies on. The FY 2025 National Defense Authorization Act (NDAA) restricted the DoD from funding fundamental research collaborations between US higher education institutions and certain foreign academic institutions, including those with ties to China.[5] Although it was removed at the eleventh hour from the 2024 NDAA, the proposed BioSecure Act was another example of the growing ambitions of the decoupling movement; at one point in its development the act's text would have forced a complete divorce between federally funded US pharmaceutical companies and Chinese services firms, which produce over 40 percent of the world's active pharmaceutical ingredients. This legislation would have shattered supply chains of the global pharmaceutical industry. While removal of that particular text might be interpreted as a temporary rebuke to that movement, it in no way defeated it. Investment flows are similarly bifurcating, with US-led initiatives like the Indo-Pacific Economic Framework for Prosperity (IPEF) and China's Belt and Road Initiative (BRI) offering competing visions for the region's economic development.

The defense sector is another area where exclusivity is becoming difficult to avoid. US arms sales and security pacts increasingly come with restrictions on using Chinese equipment, while China has its own growing market for military technology. Some countries,

like Singapore and the Philippines, have diversified defense imports, but very little of those imports comes from China. For nations like Indonesia and Malaysia that do have exposure to both defense ecosystems, maintaining access to both sources of military technology and training could become increasingly complex as the United States and China erect higher barriers to protect their most advanced weapons.

Fragmenting Ecosystems: The New Geography of Dependency

Global decoupling is no longer abstract—it's being enforced through industrial policy, export restrictions, AI model controls, and data center scrutiny. The US Department of Commerce has added numerous Chinese companies, including Huawei and Semiconductor Manufacturing International Corporation (SMIC), to its Entity List, which subjects foreign organizations and individuals listed on it to specific license requirements and restrictions on the export, reexport, and in-country transfer of sensitive and/or dual-use technologies. From the Chinese side, American chipmakers have been subjected to retaliatory security reviews, such as that imposed upon Micron in 2023, which was followed by market restrictions.[6] In late 2024, a group of industry groups including the China Association of Communication Enterprises announced their view that US chips "are no longer safe" and encouraged Chinese companies to procure chips domestically.[7]

When Chinese company DeepSeek launched its open-source DeepSeek R-1 model in January 2025, on the same day as Donald Trump's inauguration, Washington responded with an investigation that included scrutiny on Singapore, aiming to discern whether DeepSeek obtained access to banned hardware by transhipments through the city-state. Malaysia's data center industry been on a rapid growth trajectory since 2019, with US companies including Amazon, Google, and Microsoft and Chinese companies like Huawei and ZData making significant investments in the country.[8] However, Biden-era restrictions on Chinese access to high-end AI chips and threatened moves to cut Chinese access to US cloud services providers have created a fraught environment for customers of these data centers and their operators, a trend carried forward during the second Trump administration.[9]

Growing bifurcation in digital finance and payment systems also threatens to divide the region. Central banks in China, Hong Kong, Thailand, the United Arab Emirates, and Saudi Arabia are collaborating on mBridge, which enables instant, real-time cross-border payments using central bank digital currencies (CBDCs). While it differs in its core technology from SWIFT, the secure global messaging system that allows banks to communicate payment instructions to each other, mBridge is held up as an alternative to financial systems perceived as Western-dominated that have been used in sanctions. Its association with the BRICS only serves to accentuate the divide.[10]

The Strategic Dilemma: Choose or Be Chosen

While Southeast Asia's leaders continue to insist they won't choose sides, the structure of the global economy is forcing that choice on them. The cost of cross-system cooperation is rising; infrastructure can no longer plug seamlessly into both ecosystems, foreign investment is increasingly conditional, and academic partnerships now come with national security baggage. In this future, countries may find themselves locked into mutually exclusive technological and economic ecosystems, with limited opportunities for engagement across the divide. This risks stifling innovation and reducing the efficiency of global supply chains, harming growth

prospects for emerging markets. Southeast Asian companies, and those companies seeking to invest in the region, face increasing legal risks when doing business across the divide, especially in sectors that are affected by US export controls or Chinese anti-sanctions laws.

The exclusivity driven by decoupling could exacerbate inequality within Southeast Asia itself. Wealthier countries like Singapore may have the institutional capacity and strategic dexterity to operate in both systems, but others may find themselves squeezed, their choices constrained not by preference, but by design. Less developed countries could find themselves marginalized or overly dependent on a single power.

What Southeast Asia Can Do

To preserve agency, Southeast Asia must act decisively along three strategic lines of effort.

1. **Diversify partnerships:** Continue to deepen ties with middle powers, including India, and blocs such as the EU and the Gulf states to reduce exposure to either Washington or Beijing. The Regional Comprehensive Economic Partnership (RCEP) and Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), already high priorities for many regional states, will become only more relevant as countries seek the resilience that comes with diversified trading relationships. The experiences of those countries most reliant on the US market for trade (Vietnam, for example) which were most vulnerable to tariff pressure and which found themselves targeted by the Trump administration in early 2025 are likely to remain a cautionary tale against economic overdependence.

2. **Build regional resilience:** Strengthen intra-ASEAN trade. While ASEAN has traditionally observed an unspoken ceiling on its ambitions for regionalization, perhaps this new reality will provide impetus for increasing the coherence of the region's economic and tech regulation. Many refer to ASEAN as the world's "fifth largest economy" when it is in fact ten disparate markets, unlike the EU's single market. Offering companies a simpler, streamlined regulatory environment would reduce compliance burdens and operating costs, incentivizing more foreign direct investment. Lowering the 3,200 non-tariff barriers among ASEAN member states would boost the region's competitiveness and offset external volatility with intraregional trade.

3. **Assert regional digital sovereignty and harmonize regulation:** Push for multilateral norms on data governance, AI, and biotech that reflect Southeast Asian priorities rather than importing models from abroad. ASEAN's ongoing Digital Economy Framework Agreement (DEFA) negotiations are an opportunity for the region to lead on progressive digital policy. Successful creation of a legally binding regional digital agreement would boost the region's digital economy and put ASEAN into the driver's seat on global digital policy as a rule maker, rather than a rule taker. By shaping its own digital rules, ASEAN could avoid dependency on either Washington's tech-stack standards or Beijing's digital authoritarian template—preserving its regulatory sovereignty while remaining globally competitive.

A Narrowing Path

For Southeast Asia, the key challenge of the past two decades has been to preserve strategic autonomy while maximizing the benefits of engagement with both the United States and China. But most Southeast Asian states had the advantage of being courted by both sides and in most areas had significant freedom to choose between the two without fear of retaliation. As economic fragmentation hardens, Southeast Asia risks being not just a theater for great power competition, but its front line. The region must adapt swiftly to avoid becoming collateral damage in a contest it never asked to join.

Ultimately, the region's ability to navigate the growing divide will depend on the willingness of both Washington and Beijing to respect the aspirations of their Southeast Asian partners. While the United States and China may not explicitly demand allegiance, their policies are creating a world where neutrality is unsustainable. If Southeast Asia fails to act, the region could find itself trapped in a tech Cold War, split between incompatible systems, with diminished leverage and eroding sovereignty. If it acts, it has the potential to become the world's most dynamic bridge economy—resilient, neutral, and indispensable.

Endnotes

[1] *Bohdan Kukharskyy, Gabriel Felbermayr, Oliver Krebs, and Peter Eppinger, "Decoupling From Global Value Chains", VoxEU, February 17, 2021. https://cepr.org/voxeu/columns/decoupling-global-value-chains*

[2] *Cong Cao, Richard P. Suttmeier, and Denis Fred Simon, "China's 15-Year Science and Technology Plan", Physics Today, December 2006, https://china-us.uoregon.edu/pdf/final%20print%20version.pdf*

[3] *James McGregor, U.S. Chamber of Commerce, "China's Drive for 'Indigenous Innovation'", July 2010, https://jamesmcgregor-inc.com/books/chinas-drive-for-indigenous-innovation-a-web-of-industrial-policies/; Yuan Yang and Nian Liu", Beijing orders state offices to replace foreign PCs and software", Financial Times, December 9, 2019; Liza Lin, "China Intensifies Push to 'Delete America from Its Technology'", Wall Street Journal, March 7, 2024. https://www.wsj.com/world/china/china-technology-software-delete-america-2b8ea89f*

[4] *Ross Douthat, "Globalization is Over. The Global Culture Wars Have Begun", New York Times, April 8, 2022. https://www.nytimes.com/2022/04/08/opinion/globalization-global-culture-war.html*

[5] *U.S. House of Representatives, "Text of the National Defense Authorization Act for Fiscal Year 2025", December 7, 2024. https://docs.house.gov/billsthisweek/20241209/RCP_HR5009_xml%5b89%5d.pdf*

[6] *The Straits Times, "China Says U.S. Chipmaker Micron Failed Security Review", May 21, 2023. https://www.straitstimes.com/asia/east-asia/china-says-us-chipmaker-micron-failed-security-review*

[7] *Eduardo Baptista and Brenda Goh, "US Chips 'Are No Longer Safe,' Chinese Industry Bodies Say in Latest Trade Salvo", Reuters, December 4, 2024. https://www.reuters.com/technology/chinese-firms-should-diversify-chip-sources-internet-society-china-says-2024-12-03/*

[8] *Dan Swinhoe, "Malaysia's Tropicana Sells Land in Johor to ZData for Data Center Project", Data Center Dynamics, October 10, 2024. https://www.datacenterdynamics.com/en/news/malaysias-tropicana-sells-land-in-johor-to-zdata-for-data-center-project/*

[9] *Gregory C. Allen, "Choking Off China's Access to the Future of AI", Center for Strategic and International Studies, October 11, 2022. https://www.csis.org/analysis/choking-chinas-access-future-ai; Reuters, "U.S. Set to Restrict China's Access to Cloud Computing", July 4, 2023. https://www.reuters.com/technology/us-set-restrict-chinas-access-cloud-computing-wsj-2023-07-04/*

[10] *Ledger Insights, "BIS hands over mBridge CBDC payment system, after BRICS controversy", October 31, 2024. https://www.ledgerinsights.com/bis-hands-over-mbridge-cbdc-payment-system-after-brics-controversy/*

The Quad's Biotech Opportunity

By Dr. Chris Li

The Next Frontier of Strategic Competition

Biotechnology is poised to be one of the most transformative technologies of the 21st century. In the decades ahead, biotech—the powerful set of tools that harness biological processes and structures for a wide range of applications—harbors the vast potential to revolutionize medicine, reshape the global economy, disrupt national security, and transform industry and energy. Unlike chips that power advanced AI algorithms, however, biotechnology is an expansive and diverse domain that spans a multitude of modalities, including mRNA vaccines, gene editing, DNA sequencing and synthesis, engineered proteins, and the frontiers of neuroscience. Applications of biotechnology range from cutting-edge therapeutics for cancer and gene therapies that can cure devastating diseases to methods for bolstering agricultural capacity to ensure more resilient food sources across the developing world; biotechnology can enable destructive platforms for the engineering of deadly viruses and helpful tools for surveilling the global health landscape to enable early detection of novel pathogens. Given these consequential stakes for economic power and international security, the coming decades will bear witness to a fierce competition in biotechnology, where the geopolitical stakes are profound.

If anything, the COVID-19 pandemic made vivid both the disruptive and constructive effects of biotechnology. COVID upended global economies for multiple years; even deadlier viruses may wait over the horizon, including those that could potentially be developed by malign actors with the latest biotech capabilities. (Indeed, the spread of SARS-CoV-2 itself engendered a multiplicity of hypotheses about its origins—from natural occurrence to laboratory leak to even an engineered "gain of function" design.) At the same time, the rapid development of mRNA vaccines saved millions of lives and underscored the breathtaking speed with which novel modalities are emerging and the promise of biotechnology as a solution to crises of global scale. But perhaps most significantly, the pandemic made clear that despite its important use for global humanitarian purposes and public health, biotech has become a defined arena of global competition, with profound geopolitical consequences for nations. Advances in gene therapies are offering unprecedented treatments for diseases, while synthetic biology—driven by tools in protein design and genetic engineering—is unlocking new ways for generating fuel, chemicals, and crops. Meanwhile, the convergence of biology with AI and large data sets (of genomic data across populations, for example) is accelerating discoveries in drug development, neuroscience, and regenerative medicine.

Yet the story of biotech's trajectory is only in its early chapters. The many layers of the human genome remain partially understood, and cellular engineering is in its infancy. The nations that master these frontiers will not only dominate economic growth but also control the fundamental building blocks of life itself—technologies that can enable the extension of lifespan[1], reprogramming of cells[2], and selection of traits in offspring.

While much of the emerging biotech race will unfold between the United States and China, two great powers locked in a fierce Thucydidean rivalry[3] for dominance in all domains of national power, Washington does

not need to compete alone. The Quad framework—which comprises the United States, Japan, India, and Australia—offers a strategic platform for biotech collaboration among some of the closest partners in the Indo-Pacific region.

The potential for the Quad as a multilateral grouping to align foundational strengths in research, manufacturing, clinical trials, and biosecurity is promising. Leveraged to their full capacity, this cohort of states could ensure that biotechnology's future remains shaped by the norms and values of free, democratic societies. Moreover, each of the Quad countries already possesses innate structural advantages that make intentional and purposeful cooperation not only viable but prudent. From India's vigorous biomanufacturing based, undergirding enormous production capacity, to Japan's vibrant research ecosystem, these four nations converge with preexisting and complementary strengths that could easily be amplified by synergy. These reinforcing strengths aren't just theoretical. They've been demonstrated as effective force multipliers already. During the COVID-19 pandemic, the Quad Vaccine Partnership, formed in 2021, coordinated efforts by all four countries to deliver nearly 800 million vaccines around the world, while also liaising closely with local health agencies in each respective capital.[4] More can be done. This paper outlines key areas where, building on existing initiatives, the Quad may be able to play a serious and possibly decisive role in stimulating joint biotech development while sustaining international leadership on global health security and biotech innovation.

The Biotechnology Imperative and an Emerging Bio-Economy

The life sciences underpin an emerging bioeconomy that will significantly contribute to comprehensive national power in the 21st century. According to the U.S. National Security Commission on Emerging Biotechnology's 2025 report, advances in the biotech sector are expected to drive trillions of dollars in economic growth over the next few decades.[5] Unlike semiconductors, which are already deployed across economic sectors and widely integrated into global supply chains, the story of biotech is still in its infancy. The nations that lead in biotech will not only garner economic advantages but also achieve control of critical sectors like pharmaceuticals, agriculture, and even military and defense applications.

Moreover, biotech's dual-use nature (enabling applications in both the civilian and military domains) means it will impinge upon issues of macroeconomics and national security—with serious implications for both.[6] Leadership in biotech will determine the ability to combat future pandemics, enhance food security through genetically modified crops, and even potentially shape the future of warfare through bioengineered materials (and even soldiers) as well as medical treatments on the battlefield. In short, this is not a domain the United States and its allies can afford to cede to strategic competitors.

The Quad's Comparative Advantage in Biotechnology

The four Quad nations each possess unique attributes of their economies, societies, and industrial bases and simultaneously complementary strengths in research, manufacturing, and regulation that make closer coordination on biotech a singular opportunity. At first approximation, policymakers would be wise to identify—and act upon—key areas where closer alignment and coordination among Quad countries could yield significant advantages and impact over the long term, particularly for strategic competition.

Talent and Research Collaboration

While it's not all that's required, scientific talent—along with a strong biotech workforce and capabilities— is the backbone of biotech innovation. Fundamental breakthroughs in discovering novel proteins, genes, pathways, and targets drive pharmaceutical development. Without discovery and innovation, new commercial tools and technologies cannot be developed. Despite the importance of diffusion and application in any domain of technology, basic discovery still serves as a foundation. Here, the Quad countries share enormous advantages. Japan has long been a global leader in biomedical research, with numerous institutions and scientists at the forefront of regenerative medicine, stem cell research, and neurobiology, for example. India's rapid expansion and improvement of STEM education, producing over 2.5 million STEM graduates annually, and its colossal population and workforce make it a rising biotech powerhouse.[7] Meanwhile, Australia's clinical research sector and the United States' dominance in biotech startups and venture funding create a formidable coalition. Quad nations could expand joint PhD and postdoctoral programs (building off programs like the Quad fellowship), establish biotechnology research exchanges, and invest in collaborative academic networks. And in an era where Federal funding for basic science is in a period of transition, a global coalition would provide stability and balance across the four partner nations. Leveraging talent mobility among Quad nations, therefore, could significantly accelerate biotech discoveries and strengthen regional expertise.[8]

Biomanufacturing and Supply Chain Resilience

Realizing the value of innovation in biotech will depend on the ability to scale production and manufacturing. As political scientist Jeff Ding has argued, innovation must be complemented by diffusion, the spread and adoption of new technologies. The countries that adopt, scale, and diffuse new technologies gain more in their national power than those who merely introduce major innovations.[9] As with semiconductors, mere discoveries and innovative advances in capability and potential—without a corresponding increase in the ability to manufacture at scale and at efficient costs—are insufficient for a country to maintain its national lead.

Here again, the Quad can play a role. India is already a global leader in vaccine manufacturing and is home to major producers like the Serum Institute of India, which produces over 4 billion vaccine doses annually—accounting for almost half the world's doses.[10] The United States and Japan have robust biotech R&D sectors but are less competitive in biomanufacturing at cost effectiveness and scale. Indeed, in recent years in the United States, significant attention has focused on the need for competitive domestic biomanufacturers (often termed contract development and manufacturing organizations, or CDMOs) that can produce assets for early- and late-stage biotech development. While Chinese firms like WuXi AppTec have dominated this space, the United States' ability to compete has not been as effective. Closer U.S.-Indian collaboration could significantly enhance the ability of US biotech firms to manufacture at greater scale and efficiency.

Additionally, U.S. drug supply chains—especially for small-molecule drugs (that make up a majority of the medicines everyday Americans consume daily)—are heavily dependent on China. The United States currently imports an overwhelming majority of its drugs from China, or is reliant on Chinese-produced active pharmaceutical ingredients (APIs) and key starting materials (sometimes this is an undercount, as the U.S. also imports from other countries that, in turn, source from China)—a vulnerability that if one day exploited would cripple American pharmacies as

critical drugs many Americans depend on daily would be subject to shortages. As COVID made vivid, the U.S. supply chain for critical items is deeply integrated with the global economy and in many cases vulnerable to disruption. As many have argued, a Quad-backed biomanufacturing hub in India could secure resilient supply chains for critical pharmaceuticals, reducing dependency on a single source and strengthening supply chain resilience.[11]

Clinical Trials and Regulatory Harmonization

Given a large swath of biotech applications lie in the pharmaceutical sector, conducting large-scale human clinical trials is essential for continued advancement and deployment of biotech, particularly in fields like cancer therapies and gene editing. For the most promising therapeutic applications in medicine, randomized clinical trials are a crucial component of the R&D process and required for a product to ascend the value chain. Particularly for many global pharmaceutical behemoths, multiregional trials are even more important—as they seek to export to markets around the world. In this area, Japan's aging population makes it an ideal location for clinical research on age-related diseases, while Australia has a robust clinical trial ecosystem with mature and effective regulatory oversight. A Quad initiative to harmonize clinical trial protocols and data-sharing mechanisms could accelerate the approval and market adoption of new therapeutics and ensure that rigorous regulatory standards shape global biotech norms.

Biotech Standards and Ethics

From gene editing to synthetic biology, the breathtaking speed and scale of biotech innovation has also increasingly given rise to greater ethical and regulatory concerns. The Quad has an opportunity to establish responsible norms in emerging areas where ethical lines remain undefined. The 1975 Asilomar Conference, a gathering of scientists concerned with the potentially destabilizing effects of their innovations, set early guidelines for recombinant DNA, demonstrating that the scientific community has at least some ability to self-regulate (though it may not be sufficient alone).[12] However, today's biotechnology landscape is far more globalized and democratized than it was in the 1970s. The Quad could spearhead an "Asilomar 2025" or host any number of other convenings of biotech leaders, inviting the broader international community to establish ethical guidelines on genomic engineering, synthetic biology, and neurotechnologies.

Biosecurity and Biosurveillance

Preventing the misuse of biotechnology—by state actors, non-state actors, and even rogue scientists—is an equally important and intractable challenge. From a national security perspective, it is as urgent as harness innovation's promises. Particularly with the convergence of AI and biology, biosecurity should become a greater concern to policymakers—yet few private sector firms in the industry are closely focused on this issue. In short, bioconvergence, biosecurity, and bioresilience are mutually reinforcing. The Quad could lead in biosurveillance for emerging diseases, pathogen synthesis screening, and preventing bioterrorism. A coordinated biosecurity framework would have the capacity to enhance the ability to detect and respond to pandemics, building on the success of previous Quad collaborations on COVID-19 vaccine distribution.

The Quad as a Strategic Platform for Biotechnology Leadership

Given the profound consequences and strategic importance of biotech as a domain of national power, the United States and its allies should prioritize the maintenance of leadership in the field. A unique

and powerful multilateral grouping of like-minded nations, the Quad presents an optimal opportunity for biotech collaboration because its members combine technological prowess with shared values and a commitment to open, rules-based innovation. Unlike bilateral alliances, the Quad provides a multilateral structure that can scale investments, facilitate talent flows, and promote regional stability. During the Biden administration, the Quad attained unprecedented prominence, with a series of high-level gatherings at multiple levels of government. Indeed, the 2024 Quad Leaders' Summit underscored the importance of strengthening biotech ecosystems among member states.[13]

The second Trump administration is well-positioned to build on previous accomplishments and make biotech a greater priority going forward. And there are optimistic signals. On the first full day of the Trump administration, newly minted Secretary of State Marco Rubio convened a meeting of the Quad foreign ministers, his first major diplomatic engagement.[14] President Trump's earliest meetings indicated a renewed focus on U.S.-India and U.S.-Japan bilateral relations, with both Japanese Prime Minister Ishiba and Indian Prime Minister Modi welcomed to the White House within weeks of Trump's assuming office. Despite tensions between the U.S. and many of its allies derived from President Trump's ongoing global tariff campaign, there thus far appears to be a significant foundation upon which to sustain—and indeed expand and deepen—the Quad framework.

The key challenge is moving from high-level commitments to concrete initiatives. A Quad Biotechnology Initiative could formalize cooperation through:

- a Quad Biotech Research Fund to support joint projects
- a Quad Biosecurity Agreement to prevent misuse of emerging technologies
- a Quad Biomanufacturing Consortium to establish resilient supply chains
- a Quad Regulatory Forum to align standards on clinical trials and genomic ethics.

A Call to Action

The Quad presents a unique opportunity for the United States to advance its competitiveness in biotechnology. Like many technological domains, biotech is highly globalized, with countries—particularly in Asia—demonstrating success in many dimensions of biotech innovation. The Quad offers a distinct, non–security-focused multilateral framework that assembles a key group of critical economies with distinct strengths in basic science, manufacturing, education and talent, and private sector commercialization. Combined, these four countries possess singular potential not only to develop but to deploy biotechnologies at scale and with economic efficiency. Moreover, because it is not merely a security partnership, but an arrangement that encompasses economic growth, education, and even norms and rules, the Quad offers advantages as a platform for increasing biosecurity resilience as well as enhancing standards and ethics. These countries will not only be key drivers of biotechnology but key consumers, stewards, and markets for biotech products as well. Biotech leadership will shape the future of national power, economic growth, and health security. The Quad has the expertise and strategic alignment to lead in this domain. Now is the time to act.

Endnotes

[1] Kenyon, C., Chang, J., Gensch, E. et al. "A C. elegans mutant that lives twice as long as wild type", Nature 366, 461–464 (1993). https://doi.org/10.1038/366461a0

[2] Takahashi K, Yamanaka S. "Induction of pluripotent stem cells from mouse embryonic and adult fibroblast cultures by defined factors", Cell. 2006 Aug 25;126(4):663-76. doi: 10.1016/j.cell.2006.07.024. Epub 2006 Aug 10, PMID: 16904174.

[3] Belfer Center for Science and International Affairs, Harvard Kennedy School, „Thucydides's Trap Case File". https://www.belfercenter.org/programs/thucydidess-trap/thucydidess-trap-case-file

[4] Indo-Pacific Centre for Health Security, "Quad Vaccine Partnership". https://indopacifichealthsecurity.dfat.gov.au/covid-19-vaccine-access/quad-vaccine-partnership

[5] Abigail Kukura, "National Action Plan for U.S. Leadership in Biotechnology", Special Competitive Studies Project, April 2023. www.scsp.ai/wp-content/uploads/2023/04/National-Action-Plan-for-U.S.-Leadership-in-Biotechnology.pdf. See also U.S. National Security Commission on Emerging Biotechnology, "Charting the Future of Biotechnology", U.S. Congress, April 2025. https://www.biotech.senate.gov/final-report/chapters/

[6] Center for a New American Security, "New CNAS Report Outlines Strategy to Secure U.S. Biotechnology Leadership", January 15, 2024. www.cnas.org/press/press-release/new-cnas-report-outlines-strategy-to-secure-u-s-biotechnology-leadership. See full report: Chilukuri & Kelley, "Biopower: Securing American Leadership in Biotechnology" (CNAS, January 2025). https://www.cnas.org/publications/reports/biopower

[7] Julie Heng and Yutong Deng, "Innovation Lightbulb: Not Just Attracting But Retaining International STEM Students", Center for Strategic and International Studies, April 11, 2025. https://www.csis.org/analysis/innovation-lightbulb-not-just-attracting-retaining-international-stem-students; Shravishtha Ajaykumar, "The Quad's Contribution to Revolutionising Biotechnology Strategies", Observer Research Foundation, December 13, 2023. www.orfonline.org/research/the-quad-s-contribution-to-revolutionising-biotechnology-strategies

[8] Saurabh Todi, Shambhavi Naik, Dirk van der Kley, and Daniel Pavlich, "The Quad Should Commit to a Biomanufacturing Hub in India", Australian Strategic Policy Institute, May 11, 2023. www.aspistrategist.org.au/the-quad-should-commit-to-a-biomanufacturing-hub-in-india/

[9] Jeffrey Ding, "The Innovation Fallacy", Foreign Affairs, August 19, 2024. https://www.foreignaffairs.com/china/innovation-fallacy-artificial-intelligence

[10] Ministry of Health and Family Welfare, "Union Health Secretary addresses Annual India Leadership Summit organised by the US-India Strategic Partnership Forum in New Delhi", October 14, 2024. https://www.pib.gov.in/PressReleseDetailm.aspx?PRID=2064818#

[11] Todi, Naik, van der Kley, and Pavlich, "The Quad Should Commit".

[12] Berg, P. "Asilomar 1975: DNA modification secured", Nature 455, 290–291 (2008). https://doi.org/10.1038/455290a

[13] The White House, "Fact Sheet: 2024 Quad Leaders' Summit", Biden White House Archives, September 21, 2024. bidenwhitehouse.archives.gov/briefing-room/statements-releases/2024/09/21/fact-sheet-2024-quad-leaders-summit/

[14] U.S. Department of State, "Joint Statement by the Quad Foreign Ministers", January 21, 2025. https://www.state.gov/joint-statement-by-the-quad-foreign-ministers

Invisible Highways: Leveraging Maritime Domain Awareness for Subsea Cable Resilience

By Dr. Pratnashree Basu, Takuma Matsu, Natsuki Momiji, and Dr. Bich Tran

Introduction

In an Indo-Pacific where strategic tensions and digital interdependence collide, the resilience of subsea cables will define both economic security and strategic stability. These cables form the backbone of global digital connectivity, transmitting communications and data worldwide and remain highly vulnerable to both natural and man-made disruptions, including accidental damage, and sabotage (besides also being susceptible to espionage). Subsea cables in the Indo-Pacific are particularly at risk in geopolitical flashpoints across the region, such as the South and East China Seas, the Taiwan Strait, and the Malacca Strait. China's alleged tampering with undersea infrastructure raises concerns for regional actors about the use of maritime infrastructure as a tool for hybrid warfare.[1]

As integrated surveillance and real-time monitoring of subsea cables does not exist, leveraging Maritime Domain Awareness (MDA) to enhance subsea cable resilience has become an urgent necessity. This paper explores the evolving threats to subsea cables, the role of MDA in protecting them, and existing international cooperation mechanisms—such as SeaVision, IORIS, and the Quad's Indo-Pacific MDA initiative— in the broader context of developing global resilience for subsea cables. It concludes with recommendations for a comprehensive resilience framework in the Indo-Pacific.

The Digital Era's Dependence on Subsea Cables

As digital transformation accelerates, subsea cables have become increasingly important. Over 99 percent of global communications rely on subsea cables, which now exceed 1.4 million kilometres worldwide as of 2024.[2] In the Indo-Pacific, major cables such as APG (10,400 km), JUPITER (14,000 km), and Southeast Asia-Japan 2 (10,500 km) play a crucial role in connectivity.[3] Tokyo, Hong Kong, and Singapore serve as key data hubs. Japan has 219 data centers, for example, and 99% of Japan's international communication is carried by subsea cables.[4] The International Cable Protection Committee (ICPC) has noted that subsea cables cannot be fully hidden, armoured, or buried to protect them from all forms of interference, malicious or unintentional.[5] Given the reliance of global communications and financial transactions on these cables, any disruption can have immediate and far-reaching consequences.

Subsea cable disruptions lead to both direct and indirect economic losses. The direct financial burdens incurred in cable repair are estimated to be between $1 million and $3 million per incident.[6] However, these direct costs are overshadowed by the indirect financial impact, which is much harder to quantify. Subsea cables facilitate an estimated $10 trillion worth of financial transactions daily, making any delay in data transmission potentially catastrophic for international trade, banking, and foreign currency exchanges.[7] A disruption lasting even a few hours can ripple through

global markets, delay critical financial transactions, and hinder cross-border trade, affecting businesses and governments alike.

Despite growing interest in alternative communication technologies such as low-orbit satellites, subsea cables remain irreplaceable as the primary infrastructure for global data transmission. While satellites can provide partial redundancy, they lack the capacity, reliability, and speed of fiber-optic cables. In 2024, subsea cables still carried 95 percent of international data traffic, a slight decrease from 97 percent in 2012—demonstrating that they have maintained their dominant role despite advancements in satellite communication.[8] The Indo-Pacific region, particularly Southeast Asia, has been witnessing a surge in data center investments, further emphasising the critical role of subsea cables in supporting regional digital economies. Singapore alone hosts over 100 data centers, accounting for 60 percent of Southeast Asia's total data-center capacity, reinforcing its position as a regional digital hub.[9] However, this dominance may not last indefinitely, as other Southeast Asian nations, such as Malaysia, Indonesia, and Vietnam, are expanding their digital infrastructure and subsea cable investments. The rapid growth in artificial intelligence (AI)-driven applications and cloud computing will drive unprecedented demand for high-speed data transmission; a resilient subsea cable infrastructure is necessary to sustain this expansion.

Threats and Incidents of Subsea Cable Damage

Subsea cables are physically vulnerable. Most cable damage is accidental, with the primary causes including fishing activity, ship anchors, and natural disasters. Fishing activity is one of the major sources of damage, as trawling nets and fishing gear frequently snag and sever cables.[10] Ship anchors also pose a significant risk, with large vessels' anchors dropped in cable-dense areas often disrupting or breaking cables.[11] The Indo-Pacific is particularly vulnerable to natural stresses due to its location along the Pacific Ring of Fire, a geographically active zone where frequent seismic activities, including earthquakes and undersea volcanic eruptions, pose significant threats to subsea infrastructure. Additionally, severe storms and strong ocean currents may shift cables, exposing them to further risks.[12]

Geopolitical tensions in the Indo-Pacific have raised fears of intentional sabotage. On February 2 and 8, 2023, subsea cables between Taiwan and the Matsu Islands were severed in two separate incidents, with the damage on the 8th causing significant disruptions to communication and banking services.[13] This prompted Taiwan to accelerate efforts to establish satellite-based communication systems as an emergency backup, engaging foreign providers such as OneWeb to enhance redundancy. Taiwan's Minister of Digital Affairs at the time, Audrey Tang, emphasised that Taiwan must ensure continuous connectivity with the world—even in the event of intentional cable sabotage during a crisis.[14] More recently, in January 2025, a vessel crewed by Chinese nationals damaged a cable off northern Taiwan, escalating political tensions.[15] In the South China Sea, Vietnam suffered a series of cable disruptions from 2023 to mid-2024, leaving all five of its major international connections nonfunctional. Amid these incidents, the United States warned Vietnam that new cables might be vulnerable to sabotage, based on intelligence assessments.[16] Moreover, media reports that the Chinese authority granted patents for some undersea cable-cutting equipment and methods have raised concerns about their potential applications.[17]

Seeing similar risks from hostile state actors in European waters, NATO established the Critical Undersea Infrastructure Protection Centre (CUI) in 2023,

enhancing monitoring and response in the Baltic Sea.[18] The EU has also launched an action plan to safeguard subsea infrastructure, strengthening both surveillance and coordination.[19] These efforts by NATO and the EU to protect subsea infrastructure in Europe highlights the lack of comparable mechanisms in the Indo-Pacific and provide potential models for enhanced multilateral cooperation in the region.

Maritime Domain Awareness for Subsea Cable Protection

In view of these multifaceted threats to subsea cables, MDA plays a crucial role in protecting these vital lines. MDA encompasses a comprehensive understanding of activities within maritime environments that affect security, safety, economic interests, and environmental conditions. While MDA capabilities traditionally focus on coastal defence, port security, shipping management, illegal fishing prevention, and environmental monitoring,[20] they can be effectively leveraged to protect subsea cable infrastructure across prevention, response, and mitigation phases.

MDA tools enhance preventive security by monitoring vessels, detecting abnormal behavior, and alerting relevant authorities. These systems can identify vessels that deviate from established shipping routes, loiter near subsea cable corridors, or engage in unauthorized activities, triggering appropriate security responses.

Given the extensive geographical coverage of subsea cables, zone-specific MDA applications are essential for effective monitoring. At cable landing sites, surveillance cameras provide constant oversight. Within territorial waters, a layered defence approach incorporates patrol vessels, coastal radar systems, and underwater acoustic monitoring. Strategic submarine deployment serves dual purposes by providing surveillance capabilities while deterring deliberate sabotage attempts. For broader protection across Exclusive Economic Zones and international waters, different MDA tools address both cooperative and noncooperative vessels. Cooperative vessels are tracked through Automatic Identification System and Long-Range Identification and Tracking protocols. For noncooperative "dark vessels" that intentionally disable their signals, advanced satellite-based technologies such as Synthetic Aperture Radar and Radio Frequency detection can still identify them. Platforms such as the United States' SeaVision (part of the Quad's Indo-Pacific Partnership for Maritime Domain Awareness), Canada's Dark Vessel Detection, and New Zealand's Starboard Maritime Intelligence effectively utilize these methods.[21]

In the response phase after cable disruptions occur, MDA tools facilitate precise damage location identification. Platforms such as the Indo-Pacific Regional Information Sharing system[22] enable coordinated response efforts between repair vessels, Coast Guard units, and relevant authorities. Critically, MDA tools help determine whether damage resulted from accidental circumstances or deliberate actions, providing essential evidence for potential legal proceedings against responsible parties.

In the mitigation phase, MDA capabilities inform strategic planning for new cable deployments. By analysing historical vessel traffic patterns, developers can identify and avoid high-risk areas characterized by dense shipping activity, intensive fishing operations, or frequent anchoring zones. Additionally, bathymetric data integrated within MDA systems guides optimal cable routing around unstable seabed formations and geological hazards.

The strategic implementation of zone-appropriate MDA tools would create a comprehensive security framework for subsea cable infrastructure. Rather

than developing new systems, repurposing existing MDA technologies offers a cost-effective pathway to enhance subsea cable protection.

Conclusion

As digital economies expand and technologies like AI and the Internet of Things proliferate, the demand for robust and high-capacity data transmission continues to surge, underscoring the indispensable role of subsea cables in sustaining global connectivity. However, current efforts in protecting these vital lines remain fragmented. Given the dual threats of accidental and intentional damage, the Indo-Pacific must adopt a proactive approach to subsea cable protection. QUAD, ASEAN, and regional partners should strengthen MDA through cooperation between coast guards, civilian agencies, and private sector stakeholders.[23]

MDA is at the core of securing subsea cables, providing the operational clarity and capacity needed to preempt, deter, and respond to threats. Besides elevating existing MDA tools, there is a critical need to elevate MDA's role in subsea cable security by incorporating dedicated monitoring infrastructure and advanced technological solutions, such as unmanned underwater vehicles (UUVs) and acoustic sensors.[24]

Furthermore, a comprehensive framework for subsea cable resilience is urgently required, built on three core pillars: international cooperation, interagency coordination, and public–private partnerships. International collaboration is vital, as subsea cables traverse multiple jurisdictions and international waters. Multilateral efforts can establish standardized protocols for cable protection, share information on potential threats, and coordinate responses to incidents. Countries like Japan, Australia, and the United States have enhanced subsea cable security through partnerships, regulatory measures, and strategic investments.[25] Within each country's territory, there should be clear guidelines about subsea cable–related agencies' powers and responsibilities. This will prevent negligence and enable swift response to incidents. The involvement of private sector stakeholders, who own and operate the majority of subsea cables, is vital in ensuring that commercial risk management strategies align with broader national security imperatives.[26]

In addition, regional stakeholders should consider establishing dedicated MDA fusion nodes focused specifically on monitoring subsea infrastructure. These nodes can function either as standalone centers or be embedded within existing regional frameworks such as the Information Fusion Centre (IFC) in Singapore[27] or IFC-Indian Ocean Region (IFC-IOR) in India. Fusion nodes dedicated to subsea cable security would aggregate real-time data from multiple surveillance systems—such as AIS, LRIT, SAR, and acoustic sensors—alongside geospatial cable data to monitor vessel activity near critical infrastructure. Unlike NATO's military-focused efforts, the Indo-Pacific can develop a non-military surveillance network leveraging data-sharing frameworks like DFFT (Data Free Flow with Trust). By enhancing situational awareness and enabling early threat detection, these nodes would facilitate rapid, preemptive responses to potential sabotage, significantly reducing reaction times and addressing a key vulnerability in undersea cable protection.

Another step is developing joint training programs focused on rapid response to subsea threats to enhance preparedness and interoperability among Indo-Pacific nations. These programs should encompass simulated exercises on emergency communication protocols, threat neutralization, and cable repair. Incorporating lessons from NATO's recent initiatives, such as the Maritime Centre for the Security of Critical Undersea Infrastructure,[28] and the recent EU action plan to safeguard subsea infrastructure[29] can provide

valuable insights into best practices for such training endeavours. Regular joint exercises would not only improve technical capabilities but also foster trust and collaboration, essential for a unified regional approach to subsea infrastructure security.

As the digital landscape continues to evolve, safeguarding the undersea arteries of global connectivity must remain a top priority for policymakers and stakeholders alike.

Endnotes

[1] *Gahon Chiang, "China's Subsea 'Gray Zone' Tactics", Taipei Times, January 19, 2025. https://www.taipeitimes.com/News/editorials/archives/2025/01/19/2003830451*

[2] *Phil Gervasi, "Diving Deep into Submarine Cables: The Undersea Lifelines of Internet Connectivity," Kentik, March 28, 2023. https://www.kentik.com/blog/diving-deep-into-submarine-cables-undersea-lifelines-of-internet-connectivity/*

[3] *NEC, "Asia-Pacific Gateway Cable System Operational", 2016. https://jpn.nec.com/press/201611/20161117_01.html; Submarine Cable Networks, "JUPITER Cable System Overview", 2018. https://www.submarinenetworks.com/en/systems/trans-pacific/jupiter/jupiter-cable-system-overview*

[4] *Ministry of Internal Affairs and Communication, Japan, "2024 Report on the Current State of Information and Communications"; GallagherRe, "Hidden Dangers: Undersea Cables and Mitigating Economic Risk", October 2024, https://www.ajg.com/gallagherre/news-and-insights/features/hidden-dangers-undersea-cables-and-mitigating-economic-risk/*

[5] *International Cable Protection Committee, "Government Best Practices for Protecting and Promoting Resilience of Submarine Telecommunications Cables v1.2" .*

[6] *Elina Noor, "Subsea Communication Cables in Southeast Asia: A Comprehensive Approach Is Needed", Carnegie Endowment for International Peace, December 2024. https://carnegieendowment.org/research/2024/12/southeast-asia-undersea-subsea-cables?lang=en; Worldbox Intelligence, "The Race To Build Data Centres in Southeast Asia", May 24, 2024. https://mailchi.mp/19ed0cddc11c/the-race-to-build-data-centres-in-southeast-asia*

[7] *Bianca Chan, "Wall Street's Digital Lifelines: Severed Undersea Cables Could Be a Big Problem for the Global Financial System," Business Insider, February 13, 2025. https://www.businessinsider.com/severed-undersea-cables-big-problem-wall-street-2025-2*

[8] *Submarine Telecoms Forum, "Submarine Telecoms Industry Report 2024–2025", 2024. https://issuu.com/subtelforum/docs/submarine_telecoms_industry_report_issue_13; APEC Policy Support Unit, "Economic Impact of Submarine Cable Disruptions", Asia-Pacific Economic Cooperation, February 2013. https://www.apec.org/Publications/2013/02/Economic-Impact-of-Submarine-Cable-Disruptions*

[9] *Noor, "Subsea Communication Cables in Southeast Asia".*

[10] *Gigi Onag, "2024 in Review: Submarine Cables Become a Battleground", Light Reading, December 23, 2024. https://www.lightreading.com/cable-technology/2024-in-review-submarine-cables-become-a-battleground*

[11] *See Note 10.*

[12] *Nadja Skopljak, " EU Responds to Recent Incidents With Action Plan Aiming To Bolster Security of Submarine Cables", Offshore Energy, February 25, 2025. https://www.offshore-energy.biz/eu-responds-to-recent-incidents-with-action-plan-aiming-to-bolster-security-of-submarine-cables/*

[13] *Yomiuri Shimbun Staff, "Taiwan's Matsu Islands Cut Off Due to Cable Damage", Yomiuri Shimbun, March 2, 2023. https://www.yomiuri.co.jp/world/20230302-OYT1T50368/*

[14] *數位發展部，‘唐鳳部長接受彭博電視臺采訪，說明台灣强化通訊韌性，並期待與民主夥伴聯防因應AI風險，’ 數位發展部新聞參考資料 [Ministry of Digital Affairs. "Minister Tang Feng Interviewed by Bloomberg Television on Taiwan's Enhanced Communications Resilience and Expectation to Work with Democracy Partners to Address AI Risks," Ministry of Digital Affairs Background Information]*

[15] *Focus Taiwan, "China's submarine cable maneuvering leaves Taiwan at risk: Report," July 22, 2025. https://focustaiwan.tw/cross-strait/202507220006 ; Reuters, "Taiwan-China Tensions Rise Over Undersea Cable Damage," January 9, 2025. https://jp.reuters.com/world/aiwan/5MWDNX3Y5RNO3KDQZZHMV4U52A-2025-01-09/*

[16] *Onag, "2024 in Review"; Francesco Guarascio, Phuong Nguyen, and Joe Brock, "Inside the US Push To Steer Vietnam's Subsea Cable Plans Away From China," September 17, 2024. https://www.reuters.com/business/media-telecom/inside-us-push-steer-vietnams-subsea-cable-plans-away-china-2024-09-17/*

[17] *Harry Baldock, "Chinese Engineers Patent Submarine Cable-Cutting Tech", SubTel Forum, January 14, 2025. https://subtelforum.com/chinese-engineers-patenting-submarine-cable-cutting-tech/. See also the website of Chinese National Intellectual Property Administration (CNIPA, 国家知识产权局), https://www.cnipa.gov.cn/. CNIPA has granted patents to cable-cutting technologies such as one developed by Lishui University in 2020. The South China Morning Post also reported that China Ship Scientific Research Centre and its affiliated State Key Laboratory of Deep-sea Manned Vehicles developed a deep-sea cable-cutting device which is able to cut lines at depths of up to 4,000 metres.*

[18] *NATO MARCOM, "NATO officially launches new Maritime Centre for Security of Critical Undersea Infrastructure," May 28, 2024. https://mc.nato.int/media-centre/news/2024/nato-officially-launches-new-nmcscui*

[19] *Skopljak, "EU Responds to Recent Incidents".*

[20] *Bich Tran, "Vietnam's Quest for Enhanced Maritime Domain Awareness", ISEAS, December 8, 2023. https://www.iseas.edu.sg/articles-commentaries/iseas-perspective/2023-96-vietnams-quest-for-enhanced-maritime-domain-awareness-by-bich-tran/*

[21] *SeaVision, "A Web-Based Maritime Situational Awareness Tool", US Department of Transportation, n.d. https://info.seavision.volpe.dot.gov/; MDA Space, "Dark Vessel Detection Missions," n.d. https://mda.space/dark-vessel; Starboard Maritime Intelligence, "Starboard Is the Common Operating Picture for the Maritime World", n.d. https://www.starboard.nz/*

[22] *CRIMARIO II, "IORIS: The Maritime Operational Coordination & Communications Platform for the Indo-Pacific", n.d. https://www.crimario.eu/ioris-the-maritime-operational-coordination-communications-platform-for-the-indo-pacific/*

[23] *Christy Lee, "Undersea Cables as a Source of Friction in the South China Sea", VOA News, October 11, 2024. https://www.voanews.com/a/undersea-cables-emerge-as-source-of-friction-in-south-china-sea/7819426.html*

[24] *Dimitrios Eleftherakis and Raul Vicen-Bueno, "Sensors to Increase the Security of Underwater Communication Cables: A Review of Underwater Monitoring Sensors", Sensors, Vol. 20, No. 3, 2020. https://doi.org/10.3390/s20030737*

[25] *Pratnashree Basu, "Multilateralism: Key for De-Risking Indo-Pacific Subsea Cables", Pacific Forum, July 19, 2024. https://pacforum.org/publications/pacnet-50-multilateralism-key-for-de-risking-indo-pacific-subsea-cables*

[26] *Hayley Channer, "Improving Public-Private Partnerships on Undersea Cables: Lessons from Australia and Its Partners in the Indo-Pacific", Indo-Pacific Outlook, Volume 1, Issue 2, January 17, 2024. https://manoa.hawaii.edu/indopacificaffairs/article/improving-public-private-partnerships-on-undersea-cables-lessons-from-australia-and-its-partners-in-the-indo-pacific/*

[27] *Ariel Stenek, "A Principled Approach to Maritime Domain Awareness in the Indo-Pacific", Pacific Forum, April 4, 2023. https://pacforum.org/publications/pacnet-28-a-principled-approach-to-maritime-domain-awareness-in-the-indo-pacific/*

[28] *NATO MARCOM, "NATO officially launches new Maritime Centre for Security of Critical Undersea Infrastructure".*

[29] *Nadja Skopljak, " EU Responds to Recent Incidents With Action Plan Aiming To Bolster Security of Submarine Cables".*

About the Authors

Dr. Pratnashree Basu

Dr. Pratnashree Basu is an Associate Fellow (Indo-Pacific) within the Strategic Studies Programme and the Centre for New Economic Diplomacy at the Observer Research Foundation(ORF). Her work focuses on maritime geopolitics in the Indo-Pacific, with a particular focus on the South China Sea. She also covers Japan's strategic engagement in the region. Her research delves into the geostrategic dimensions of a rules-based maritime order, maritime law and governance, maritime geopolitical developments and partnerships in the Indo-Pacific, and the politics of development cooperation.

Recently, she earned a doctoral degree in International Relations from Jadavpur University. She is also a Fellow of the Daniel K. Inouye Asia-Pacific Centre for Security Studies (2021 and 2023) and a US Department of State IVLP Fellow (2017). She is also a recipient of the Japan Foundation Indo-Pacific Partnership (JFIPP) Research Fellowship for 2025 as well as part of the German Marshall Fund of the United States (GMF) Young Strategists Forum 2025.

With over a decade of policy research experience, her work has been featured in books, monographs, and peer-reviewed journals. In addition to her research at ORF, she regularly contributes to various online and print platforms, including The Hindu Business Line, The Hindu, The Pacific Forum, 9DashLine, The Diplomat, and the East Asia Forum.

Michal Bokša

Michal Bokša works as an International Affairs Analyst at the NATO Strategic Direction-South Hub located at NATO's Joint Force Command in Naples. In the past, he worked as an Analyst at NATO's Reach-back Analytical Cell, NATO's Supreme Headquarters Allied Powers Europe, and at NATO Defence College. Michal holds a master's degree in international relations and politics from the University of Cambridge.

Dr. Maximilian Ernst

Dr. Maximilian Ernst is a lecturer at the Military Academy of the German Armed Forces in Hamburg. Maximilian's research focuses on Indo-Pacific security, in particular Chinese statecraft towards the Asia-Pacific region. He is the author of the book China's coercion of states in the Asia-Pacific region, published with the Routledge Asian Security Studies Series. Maximilian's research has appeared in journals such as the North Korean Review, Naval War College Review, Defence Studies, Journal of Current Chinese Affairs, Journal of Territorial and Maritime Studies, and the Journal of Intelligence, Propaganda and Security Studies, among others. Previously, Maximilian was a researcher at the Centre for Security, Diplomacy and Strategy (CSDS), research fellow at the American German Institute (AGI) and a Next Generation Korea Peninsula Security Specialist with the National Committee on American Foreign Policy (NCAFP).

Dr. Eyck Freymann

Dr. Eyck Freymann — a diplomatic historian and China specialist by training – has created work spanning the fields of political economy, climate policy, and national security. His first book, One Belt One Road: Chinese Power Meets the World, was published by Harvard University Press in 2021. His essays on China and other current affairs topics have appeared in the Wall Street Journal, Foreign Affairs, The Economist, Foreign Policy, and The Atlantic.

Dr. Freymann was previously a postdoctoral research fellow at the Belfer Center's Arctic Initiative and the Columbia–Harvard China and the World Program. He holds a doctorate in China studies from Balliol College, University of Oxford; master's degrees in China studies from Harvard University and St Edmunds College, University of Cambridge; and a bachelor's in East Asian history from Harvard College.

LCDR Blake Herzinger

Blake Herzinger is the Director for Asia government affairs for a large US MNC. He joined from Indo-Pacific Advisors, an independent boutique consultancy he founded monitoring political and regulatory trends in Asia for regional corporates and private equity groups. Prior to this Blake worked in strategy and operations at Twitter and spent five years as an advisor to the US Pacific Fleet in Singapore, planning and executing the Indo-Pacific Maritime Security Initiative. He spent 10 years in active duty service in the US Navy as an intelligence officer, transitioning to the US Navy Reserve in 2017. Blake has been affiliated with several thinktanks, including the American Enterprise Institute, University of Sydney United States Studies Centre, and Pacific Forum. His work is broadly focused on technology and trade, Indo-Pacific defence policy, and US security cooperation, with emphasis on maritime security and sea power. He holds an MSc in Strategic Studies from the S. Rajaratnam School of International Studies (RSIS) at Nanyang Technological University, and completed his BA in Political Science at Brigham Young University.

Agnieszka Kurzej

Agnieszka Kurzej served for a decade in the U.S. federal government at the White House, Pentagon, and USAID. She most recently served as Chief of Staff for Cyber Policy in the Office of the Under Secretary of Defense for Policy, until December 2025. She was previously Director for Western Europe at the National Security Council from 2023-2024, where she was responsible for managing the White House's relations with key European Allies. Prior to that, she was the Deputy Director for North and West Europe and Country Director for the United Kingdom and Ireland at the Pentagon (2019-2023). She joined the Department of Defense in 2017 as a Country Director for Russia, and later served as a Country Director for the Balkans (2018) and the Nordics (2019). She began her federal civil service in 2015 at the U.S. Agency for International Development (USAID) as a Presidential Management Fellow.

Prior to her government service, Agnieszka was a Brent Scowcroft Award Fellow at the Aspen Strategy Group and a paralegal in Cooley LLP's Washington, D.C. offices.

She holds a Master of Science in International Relations from the London School of Economics, and a Bachelor's from Georgetown University's School of Foreign Service. She also earned a certificate in Eurasian, Russian, and East European Studies from Georgetown and studied abroad at Sciences Politiques in Dijon, France. She speaks advanced Polish and French, as well as beginner Russian and German.

Dr. Chris Li

Chris Li is a Technology and Geopolitics Fellow at Harvard University's Belfer Center for Science and International Affairs, where he teaches and directs programming on U.S.-China relations, Indo-Pacific security, the geopolitics of Asia, and technology competition. His research interests also include Chinese domestic and elite politics, cross-Taiwan strait relations, and the nexus of biotechnology and national security, a topic on which he has led analytic projects for the U.S. government and private sector firms. Previously at the Center, Chris served on the research staff of the Avoiding Great Power War Project led by Professor Graham Allison and as executive coordinator of the China Working Group, while also contributing to the Technology and Public Purpose Project, led by former Secretary of Defense Ash Carter. Prior to joining the Belfer Center, Chris was special assistant for life sciences strategy in the Office of the Provost at Harvard and conducted research in a molecular biology lab at Massachusetts General Hospital. A proud native of New Jersey, Chris received his B.A. in biology from Harvard University and a M.A. in Global Affairs from Tsinghua University, where he was a Schwarzman Scholar. He is currently completing his PhD in biological and biomedical sciences at Harvard University.

Annes Llwyd

Annes Llwyd is a Senior Strategy Advisor at the UK Cabinet Office's National Security Secretariat. She has worked at the heart of the UK's foreign policy and national security system for nearly a decade.

Annes was part of the small team who developed and published the UK's foreign policy and national security strategy, Integrated Review Refresh, in 2023. She now leads cross-government projects to identify strategic security and geopolitical challenges, and devises new policy approaches to address them, ranging from climate security to the implications of emerging conflicts. Her previous experience includes leading diplomatic engagement teams and overseas postings, as well as more domestic-focused roles delivering legislation in the UK Parliament.

Annes' interests and particular expertise include the geopolitical competition over the energy transition and emerging technologies, the evolving nature of power and influence, the long-term future of geopolitics, and the impact of technological innovation on global security and the international order.

Originally from Wales, her first language is Welsh but she is now settled in London. She has an MA (Distinction) in Global Politics from Aberystwyth University and BA (First) in International Relations from Swansea University. She has recently graduated from the UK Civil Service's Future Leaders Scheme with a Postgraduate Certificate in Leadership & Development.

Dr Iain MacGillivray

Dr Iain MacGillivray is a full researcher at RAND Australia, specialising in defence and national security research. With more than fourteen years of experience in Australia and internationally, Dr MacGillivray's work spans government, think tanks, and academia. His research focuses on land power and military strategy, geopolitics and geostrategy, U.S. politics and security, and complex international issues in the Indo-Pacific, Middle East, Turkish politics, and Australian foreign policy.

Previously, Dr MacGillivray served in the Chief of Army's Initiatives Group within the Australian Army, where he was the chief of the Australian Army's personal researcher and deputy speechwriter. He also worked as a UK and U.S. adviser in the international division at the Department of the Prime Minister and Cabinet and was a founding member of the Australian

Strategic Policy Institute in Washington, D.C. (ASPI DC), the first Australian think tank in the United States. He participated as an Australian delegate in the 2025 German Marshall Fund U.S./Sasakawa Peace Foundation Young Strategists Forum in Tokyo. During the 2021–22 academic year, he was a Yale Fox International Fellow at Yale University and has conducted academic research and teaching at the University of Melbourne.

Dr MacGillivray earned his PhD in International Relations from the University of Melbourne in Melbourne, Australia.

Takuma Matsu

Takuma Matsu is a research fellow at the Sasakawa Foundation (SPF). He is in charge of the Future Fellowship for Okinawa III program and US-China Relations and Japan's Security program. He received an M.A. in International Relations from the Graduate School of Global Studies at Sophia University in Japan. While completing this master course, he was selected as a member of the Kingfisher Global Leadership Program. He received a B.A. in Arts from the Faculty of Foreign Languages at Dokkyo University in Japan. He worked for the Japan Ground Self-Defense Force (JGSDF) between 2006-2011 in the Northeastern Army, Reconnaissance Unit. He retired from the JGSDF in 2011. In April 2022, he began his current position at SPF.

Jiro Minier

Jiro Minier leads the Threat Intelligence Research & Analysis team at the Deutsche Cyber-Sicherheitsorganisation (DCSO), a Berlin-based cybersecurity competence center, with a personal research focus on China-nexus cyberespionage activity.

He is actively involved in the cybersecurity and technology policy debate, including as a member of the German Council on Foreign Relations' Action Group Zeitenwende, and has held prior fellowships with the European Cyber Conflict Research Initiative and the Centre for International Security at the Hertie School in Berlin.

He holds degrees in International Relations from the London School of Economics and Political Science and the University of Cambridge.

Natsuki Momiji

Natsuki Momiji is section chief of Defence Intelligence Division, Ministry of Defense, Japan. She has been analysing military trends of countries surrounding Japan with particular focus on China, North Korea and Russia. She studied abroad at Peking University, China in 2019-2021.

Dr. Masatoshi Murakami

Masatoshi Murakami is an associate professor at Kogakkan University in Japan and a visiting researcher at the Nakasone Peace Institute. Prior to his academic career, he served as a career diplomat with Japan's Ministry of Foreign Affairs, including postings in London and Beijing. He has undertaken visiting fellowships at leading research institutions, including the National Defense University of Taiwan, the Pacific Forum in Honolulu, and Tampere University in Finland.

CAPT Diana Y. Myers

Captain Diana Y. Myers, Ph.D. is the Chief Strategic Competition Intelligence Strategist for the U.S. Air Force at Osan Air Base, Republic of Korea. She previously served as a U.S. Air Force Fellow at the RAND Corporation, focusing on strategic challenges in the Indo-Pacific region. She has worked with leading

nuclear policy organizations, including the Center for Strategic and International Studies (CSIS) as a 2022 PONI Scholar, the Center for Global Security Research (CGSR) at Lawrence Livermore National Laboratory, and the Council on Strategic Risks as a Nuclear Risk Reduction Fellow. Her doctoral research examined the role of third-party intervention in nuclear contingency planning on the Korean Peninsula. She now focuses on integrating artificial intelligence and machine learning into modernizing nuclear command and control systems. Diana holds a B.S. in Political Science from the U.S. Air Force Academy and a Ph.D. in Policy Analysis from the Pardee RAND Graduate School.

Dr. Sayaka Shingu

Dr. Sayaka Shingu joined the Ministry of Foreign Affairs of Japan in 2010. As Assistant Director of Non-Proliferation, Science and Nuclear Energy Division, she is in charge of counter WMD proliferation, including the Proliferation Security Initiative and United Nations Security Council Resolution 1540. As former Assistant Director at Arms Control and Disarmament Division, she contributed to developing Japan's position on arms control affairs, including the INF Treaty and New START. She is a 2024-2027 fellow of Project on Nuclear Issues Mid-Career Cadre at CSIS, and was a 2023-2024 fellow of Next Generation of U.S.-Japan Nuclear Policy Experts at the Mansfield Foundation, a 2021-2022 fellow of the Arms Control Negotiation Academy, a 2020-2022 fellow of the Japan-US partnership program at the Research Institute for Peace and Security, and a 2013 intern of the United Nations Office for Disarmament Affairs. Sayaka has publication in Nonproliferation Review and INKSTICK media, and holds a Ph.D. in Law from Hitotsubashi University, and a M.A. in Non-proliferation and Terrorism Studies from the Middlebury Institute of International Studies at Monterey.

Dr. Bich Tran

Dr. Bich Tran (pronounced "Bik Trahn") is a Research Fellow with the Military Transformations Programme at the S. Rajaratnam School of International Studies (RSIS). Previously, she was a Postdoctoral Fellow at the Lee Kuan Yew School of Public Policy and a Visiting Fellow at the ISEAS–Yusof Ishak Institute.

She has also held non-resident or visiting fellowships with several non-Singaporean think tanks, including Verve Research (ongoing), the Center for Strategic and International Studies (CSIS), the International Institute for Strategic Studies (IISS), and the East-West Center (EWC) among others.

Dr. Tran holds a PhD in Political Science from the University of Antwerp, Belgium. Her research expertise spans grand strategy, maritime security, cybersecurity, outer space security, and other issues at the intersection of geopolitics and technology.

The views expressed herein are those solely of the author(s). GMF as an institution does not take positions.

G | M | F