



U.S.-JAPAN TECHNOLOGY AND ECONOMIC SECURITY ACHIEVING RESILIENCE IN AN ERA OF DISRUPTION

NBR

THE NATIONAL BUREAU
of ASIAN RESEARCH

Edited by Jonathon Marek and Doug Strub

NBR Board of Directors

John V. Rindlaub (Chair) Regional President (ret.) Wells Fargo Asia Pacific	Melody Meyer President Melody Meyer Energy LLC	Tom Robertson Corporate Vice President and Deputy General Counsel Microsoft
Ahn Ho-young Former Ambassador (South Korea)	Huan Nguyen Rear Admiral (ret.), U.S. Navy; Senior Advisor to Naval Sea Systems Command	Cynthia A. Watson Professor and Dean Emerita National War College
Richard J. Ellings President Emeritus and Counselor NBR (ret.)	Long Nguyen Chairman, President, and CEO Pragmatics, Inc.	Michael Wills President NBR
Jonathan W. Greenert Admiral, U.S. Navy (ret.)	Kenneth B. Pyle Professor, University of Washington Founding President, NBR	<i>Honorary Director</i>
Charles Hooper Senior Counselor The Cohen Group	Jonathan Roberts Founder and Partner Ignition Partners	George F. Russell Jr. Chairman Emeritus Russell Investments
Quentin W. Kuhrau (Treasurer) Chief Executive Officer Unico Properties LLC		

NBR Chairs and Counselors

Charlene Barshefsky U.S. Trade Representative (ret.)	Richard J. Ellings NBR (ret.)	Roy Kamphausen NBR (Special Advisor)
Charles W. Boustany Jr. U.S. House of Representatives (ret.)	Thomas B. Fargo Admiral, U.S. Navy (ret.)	Ashley J. Tellis Carnegie Endowment for International Peace
Norman D. Dicks U.S. House of Representatives (ret.)	Aaron L. Friedberg Princeton University	

NBR Board of Advisors

William Abnett NBR	Robert Holleyman Office of the U.S. Trade Representative (ret.)	Rajeswari Rajagopalan Australian Strategic Policy Institute (ret.)
Se Hyun Ahn University of Seoul	Mark Jones Kingswood Capital Solutions	Evans Revere Department of State (ret.)
Dennis C. Blair Admiral, U.S. Navy (ret.)	Amit Kapoor India Council on Competitiveness	Clarine Nardi Riddle Kasowitz Benson Torres LLP
Ketty Chen Taiwan Foundation for Democracy	Tariq Karim Former Ambassador (Bangladesh); Independent University	Ryo Sahashi University of Tokyo
Chun In-Bum Lt. General, ROK Army (ret.)	Heino Klinck U.S. Army/Department of Defense (ret.)	Ulrike Schaede University of California San Diego
Josh Corless ConocoPhillips	David Lampton Johns Hopkins University	Robert Scher BP
Linda Distlerath PhRMA (ret.)	Stephen Lanza Lt. General, U.S. Army (ret.)	David Shambaugh George Washington University
Nelson Dong Dorsey & Whitney LLP (ret.)	Nicholas Lardy Peterson Institute for International Economics	Benjamin Shobert Optum
Nicholas Eberstadt American Enterprise Institute	Richard Lawless New Magellan Ventures	Mike Studeman Rear Admiral, U.S. Navy (ret.)
Karl Eikenberry Former Ambassador (U.S.); Lt. General, U.S. Army (ret.)	William McCahill Department of State (ret.)	Travis Sullivan Boeing Company
Bates Gill NBR	Dewardric L. McNeal Longview Global	Alison Szalwinski The Asia Group
Clara Gillispie NBR	Meredith Miller NBR	Travis Tanner Greenpoint Group
Stephen Hanson College of William and Mary	Tami Overby Albright Stonebridge Group	Arzan Tarapore Stanford University
Harry Harding University of Virginia (ret.)	John S. Park Harvard Kennedy School	Jessica Teets Middlebury College
Mikkal Herberg University of California San Diego	Pamela Passman APCO Worldwide	Debra Waggoner Corning (ret.)
Carla A. Hills Hills & Company		Dana White Juno Collective

THE NATIONAL BUREAU *of* ASIAN RESEARCH
NBR SPECIAL REPORT #116 | FEBRUARY 2025

U.S.-JAPAN TECHNOLOGY AND ECONOMIC SECURITY

Achieving Resilience in an Era of Disruption

Edited by

Jonathon Marek and Doug Strub

This report was produced by the National Bureau of Asian Research with support from the United States–Japan Foundation.

THE NATIONAL BUREAU *of* ASIAN RESEARCH

The NBR Special Report provides access to current research on special topics conducted by the world's leading experts in Asian affairs. The views expressed in these reports are those of the authors and do not necessarily reflect the views of other NBR research associates or institutions that support NBR.

The National Bureau of Asian Research helps decision-makers better understand Asia and craft concrete, actionable policy. NBR is an independent research institution based in Seattle and Washington, D.C. We bring world-class scholarship to bear on the evolving strategic environment in Asia through original, policy-relevant research, and we invest in our future by training the next generation of Asia specialists.

Our research is conducted by a global network of specialists and tackles critical issues identified by stakeholders in anticipation of future challenges. The findings are a result of independent scholarship and do not reflect institutional perspectives. Our rigorous standards facilitate informed decision-making based on knowledge rather than ideology.

Established in 1989, NBR is a legacy organization of Senator Henry M. Jackson, who foresaw the national need for an institution to study and inform public policy on Asia in both the public and private sectors. Building on Senator Jackson's bipartisan approach, NBR engages policymakers looking for reliable Asia expertise through sustained interaction in high-trust, nonpartisan settings. Our experts and research have shaped congressional legislation and administration policies, brought issues to the top of the U.S. foreign policy agenda, and attracted worldwide media attention. We mobilize expertise on Asia for a more effective foreign policy.

NBR receives support from foundations, corporations, government (including foreign governments of allies and liberal democracies), and public agencies, and philanthropic individuals. NBR reserves the right to publish findings. We do not undertake classified or proprietary research work, and we observe policies to avoid conflicts of interest.

To download issues of the NBR Special Report, please visit the NBR website <http://www.nbr.org>.

This report may be reproduced for personal use. Otherwise, the NBR Special Report may not be reproduced in full without the written permission of NBR. When information from NBR publications is cited or quoted, please cite the author and The National Bureau of Asian Research.

This is the one-hundred-and-sixteenth NBR Special Report.

NBR is a tax-exempt, nonprofit corporation under I.R.C. Sec. 501(c)(3), qualified to receive tax-exempt contributions.

© 2025 by The National Bureau of Asian Research.

For further information about NBR, contact:

The National Bureau of Asian Research
One Union Square
600 University Street, Suite 1012
Seattle, Washington 98101

206-632-7370 Phone
nbr@nbr.org E-mail
<http://www.nbr.org>

U.S.-JAPAN TECHNOLOGY AND ECONOMIC SECURITY

Achieving Resilience in an Era of Disruption

— TABLE OF CONTENTS —

- 1 Achieving Resilience in an Era of Disruption
Saori N. Katada
- 11 Japan's Approach to Resilience and Economic Security
Yuichi Hosoya
- 21 The United States' New Search for Economic Resilience
Michael Beeman
- 33 The Strategic Role of Japan's Development Finance under the New Dimension
of Digital Infrastructure
Hiroyuki Suzuki
- 45 Japan's Cybersecurity Resilience Efforts in Collaboration with the United States
Mihoko Matsubara
- 55 Countering Economic Coercion
Mariko Togashi

THE NATIONAL BUREAU *of* ASIAN RESEARCH
NBR SPECIAL REPORT #116 | FEBRUARY 2025

Achieving Resilience in an Era of Disruption

Saori N. Katada

SAORI N. KATADA is Professor of International Relations at the University of Southern California and the Director of the Center for International Studies. She is the author of *Japan's New Regional Reality: Geoeconomic Strategy in the Asia-Pacific* (2020). She can be reached at <skatada@usc.edu>.

The belief in the benefits of economic interdependence and the prospects of commercial peace based on free trade have receded over the course of the last decade. Now, policymakers' attention is focused on weaponization of economic interdependence and business disruption, and a future is coming into view where advanced and critical technology become the sources of major national security threats and geopolitical conflicts. In the 2020s, the concerns over "economic resilience" and "economic security" have become the centerpieces of international economic relations, under which governments focus on protection of their countries' supply chains and critical infrastructure and work to secure leadership in technological competition around the world.

States encounter challenges in multiple aspects of economic resilience. One prominent manifestation comes in the form of supply chain disruptions and how to protect the economy from associated costs. In this context, economic coercion by weaponizing other countries' supply chain dependence has become a brazen tactic. Advances of digital technology and artificial intelligence (AI) in recent years have also led to an expanded set of dual-use technologies, increasingly blurring economic and security issues and introducing new challenges to economic resilience. Establishing and securing dominance in advanced technologies will be essential for maintaining leadership in the global economy, while defending the national economy from abuses of these technologies such as cyberattacks has also become a vital component of economic security.

These developments in the area of economic security have made U.S.-Japan technological and economic cooperation ever more vital to the bilateral relationship and the region as a whole. The two long-standing security allies both possess advanced technology ecosystems. They have worked on these challenges independently and occasionally in collaboration for some time as they both view China's actions with alarm. Although some aspects of their strategies toward economic resilience diverge, the common aim is focused on countering these threats without wrecking global economic activities, which has allowed both economies to thrive for the last seven decades.

This introductory essay first examines the growing risk to economic resilience and the measures being taken to tackle economic coercion. It then considers the role of digital technology and cybersecurity as they become critical features of economic security. The third section covers U.S.-Japan cooperation on collective resilience and the challenges the two countries face in achieving this objective. This introduction concludes with short synopses of the five essays in this report.

The Growing Risk of Supply Chain Disruptions and Economic Coercion

Economic interdependence stemming from cross-border trade and investment provides countless benefits—from access to affordable goods to efficient international production networks—but also exposes economies to dependency and makes them vulnerable to disruption. While the sources of disruption could be natural disasters such as the Covid-19 pandemic, wars, or major accidents, especially in key shipping routes (such as the Suez or Panama Canals), disruptions can also be intentionally deployed by major powers to achieve certain political objectives. The latter kind of disruption, called "weaponization" of interdependence, involves the use of coercive economic tools ranging from sanctions to boycotts. After China rose to become a central node of trade and investment, the Chinese government began to use these tactics to achieve its foreign policy goals, as was demonstrated more than a decade ago with its 2010 rare earth elements

embargo against Japan. As the international trade regime based in the World Trade Organization has suffered from paralysis, stakeholders must seek alternative ways to guard against economic disruption and ensure the resilience of global economic activities.

In 2020 the world experienced an unimaginable disruption of supply chains for several months during the Covid-19 pandemic. Soon thereafter, multiple political uncertainties followed, ranging from wars to canal and port shutdowns, reminding every government and business alike how vital it is to maintain supply chain “resilience.”¹ As the governments of advanced economies develop their strategies, efforts to achieve economic resilience incorporate not only the short-term defensive objective of cultivating alternative sources for production but also long-term goals such as maintaining technological autonomy and denying potential adversaries’ future dominance to reduce the number of possible threats.

One of the steps to beef up supply chain resilience is to diversify the location of production and thereby increase the number of import sources. From reshoring to friendshoring or allyshoring, the U.S. and Japanese governments—along with other like-minded partners—began to advocate relocating production facilities and import sources away from China-centric networks.² At the same time, with the increasing frequency and visibility of economic coercion (discussed in detail in the essay by Mariko Togashi), multilateral forums among the industrialized economies, including the G-7 and Organisation for Economic Co-operation and Development (OECD), began in recent years to share information between governments and develop collective policies to deter and counter economic coercion with the aim to increase the perceived costs of such behavior.

High Fences in Support of Digital Technology and Fending Off Cybersecurity Risks

Digital technology has brought tremendous benefits and considerable risks for the world. It has provided the foundational infrastructure for a thriving digital economy, enhancing efficiency and expanding commercial opportunities. However, these developments have exposed both economic and national security vulnerabilities through challenges to cybersecurity and attacks on critical infrastructure, both actual and potential (discussed in Mihoko Matsubara’s essay). Furthermore, cutting-edge technology with dual-use civilian and military applications, such as generative AI and quantum computing, has blurred the line between preparations for peacetime and war.

As it has become imperative for the United States to gain dominance in such sensitive and critical technologies, the Biden administration’s national security advisor Jake Sullivan used the phrase “small yard and high fence” to describe how the United States seeks to protect foundational

¹ The 2022 *Economic Report of the President* defines “resilience” as “the ability of supply chains to recover quickly from unexpected events.” The White House later outlined in a briefing note in November 2023 that “resilience can be achieved through better data on the structure of supply chains, investments in redundancy, greater ability to substitute between inputs, and improved communication across the supply chain.” Further discussion of how the U.S. and Japanese governments define “resilience” occurs in the first two essays. See White House, *Economic Report of the President* (Washington, D.C., April 2022), <https://www.whitehouse.gov/wp-content/uploads/2022/04/ERP-2022.pdf>; and White House, “Issue Brief: Supply Chain Resilience,” Issue Brief, November 30, 2023, <https://www.whitehouse.gov/cea/written-materials/2023/11/30/issue-brief-supply-chain-resilience>.

² Reshoring policy is defined as “the deliberate government policies to bring manufacturing from abroad to home country.” Some use “backshoring,” “onshoring,” or “inshoring” as equivalent to reshoring. See Saori N. Katada, Ji Hye Lim, and Ming Wan, “Reshoring from China: Comparing the Economic Statecraft of Japan and South Korea,” *Pacific Review* 36, no. 5 (2023). For further discussion of friendshoring, see “Remarks by Secretary of the Treasury Janet L. Yellen on Way Forward for the Global Economy,” U.S. Department of the Treasury, Press Release, April 13, 2022, <https://home.treasury.gov/news/press-releases/jy0714>.

technologies such as semiconductors and usher in the waves of digital revolution.³ Meanwhile, both the U.S. and Japanese governments are implementing measures to improve cybersecurity, protect critical infrastructure, and strengthen economic resilience, while also developing regulations and guidelines for the safe and ethical use of generative AI (see Hiroyuki Suzuki's essay in this report).

U.S.-Japan Cooperation toward "Collective Resilience"

Whether intentionally deployed as a tool of weaponization or resulting from uncontrollable factors like the Covid-19 pandemic, the world has recently experienced significant consequences arising from economies' overdependence on single points of origin for critical products and inputs. Many such points are concentrated in China following its rapid growth as a manufacturing and export hub. Furthermore, China's technological advancement in recent decades has led to potential and real threats encompassing military application of dual-use technology and other disruptive capabilities in the form of economic coercion or cyber threats. Facing this challenge, the United States began calling for decoupling from China during the first Trump administration, especially with the imposition of tariffs on multiple sets of imported goods primarily from China from 2018. These tariffs aimed to protect manufacturing jobs and industries in the United States, pursue national security goals, push China toward adopting market reforms and stronger intellectual property protections, and shrink the U.S. trade deficit with China.⁴ During these years, a primary tactic used by Japan, as one of the early targets of China's economic coercion in 2010, was to promote a China-plus-one strategy under which the government encouraged businesses to diversify their sources of imports and destinations of investments.⁵ The Covid-19 pandemic intensified the disruptions and coercive behavior by China. Beijing banned Australian exports such as wine, barley, and beef to protest the Australian government's request for further investigation into the origins of the virus in China. All these developments further heightened concerns of supply chain disruptions throughout 2020.

After being inaugurated in January 2021, President Joe Biden advocated an agenda of "foreign policy for the middle class."⁶ The foreign economic policy of the Biden administration has followed the path of the Trump era based on bipartisan support for an anti-China posture (see Michael Beeman's essay in this report), including by abandoning trade agreements and maintaining tariffs against China. When it comes to the U.S. posture toward its allies and "like-minded" countries in the efforts toward supply chain resilience, however, President Biden opened

³ "Remarks by National Security Advisor Jake Sullivan on Renewing American Economic Leadership at the Brookings Institution," White House, April 27, 2023, <https://www.whitehouse.gov/briefing-room/speeches-remarks/2023/04/27/remarks-by-national-security-advisor-jake-sullivan-on-renewing-american-economic-leadership-at-the-brookings-institution>.

⁴ A part of this came from an influential article estimating that more than two million American jobs were lost due to the sizable increase in Chinese imports into the United States between 1999 and 2011. See David Autor, David Dorn, and Gordon H. Hanson, "The China Shock: Learning from Labor-Market Adjustment to Large Changes in Trade," *Annual Review of Economics* 8, no. 1 (2016): 205–40.

⁵ Keisuke Iida, "Political Risks and Japanese Foreign Direct Investment in East Asia: A Case Study of 'China-Plus-One,'" *Korean Journal of International Studies* 13, no. 2 (2015): 383–410.

⁶ "Remarks by President Biden on America's Place in the World," White House, February 4, 2021, <https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/02/04/remarks-by-president-biden-on-americas-place-in-the-world>.

a new page of “collective resilience.”⁷ His economic team called for supply chain resilience from the early phase of his presidency with the executive order on February 24, 2021, to evaluate U.S. supply chains.⁸ From that time, the Biden administration emphasized “collective” efforts toward supply chain resilience.

The U.S. visit by Japan’s then prime minister Yoshihide Suga in April 2021 was an important event that demonstrated how the Biden administration would work to build collective resilience with its allies, as the two leaders agreed to launch the Competitiveness and Resilience (CoRe) Partnership.⁹ The U.S. and Japanese governments committed to expand and renew their countries’ partnership in critical technologies such as secure and open 5G+ networks, public health, and green growth, among other areas. Following this major step, bilateral collaboration has continued in a wide range of technological, infrastructural, and economic projects covered across this report’s essays. First, on critical digital technology and infrastructure, the U.S. and Japanese governments have agreed to support the development of Open RAN (radio access network) to establish a new network ecosystem beyond 5G with a \$4.5 billion co-investment.¹⁰ Second, the U.S. and Japanese governments signed a critical minerals agreement in March 2023 with the aim to have the five minerals (cobalt, graphite, lithium, manganese, and nickel) exported from Japan used to produce electric vehicles (EVs), which will be covered under EV subsidies of the Biden administration’s Inflation Reduction Act, enacted in August 2022.¹¹ Third, as a way to revitalize semiconductor production, the United States and Japan agreed on the Basic Principles on Semiconductor Cooperation in May 2022. To coordinate these activities, the two governments established a new bilateral policy coordination forum called the Economic Policy Consultative Committee (consisting of economic ministers and foreign ministers, dubbed as the Economic 2+2). At its first meeting in July 2022, the two parties agreed to participate in joint research in key technologies such as advanced semiconductors and to work together to secure sources of critical minerals.

Japan’s active engagement helped foster these bilateral initiatives. As a trade- and energy-dependent economy, Japan has long been familiar with the notion of economic security (see Yuichi Hosoya’s essay). Particularly since the 2010s, Japanese political leaders have been at the forefront of tackling related issues. In the mid-2010s, the Abe government promoted the “free and open Indo-Pacific” (FOIP) framework that emphasizes the rules-based order for the global economy. The Diet Members Caucus for Rule Formation Strategy, chaired by former Trans-Pacific Partnership negotiator Akira Amari, was established within the Liberal Democratic Party (LDP) in 2017 to tackle multiple economic security concerns, ranging from next-generation technology to cybersecurity. A set of LDP recommendations was later published in December 2020 in support

⁷ The term “collective resilience” was coined by Brad Glosserman and Eric Sayers in August 2020 and advanced widely by Victor Cha in two articles published in 2023. See Brad Glosserman and Eric Sayers, “‘Collective Resilience’ Is the Way to Address China Challenge,” *Japan Times*, August 14, 2020, <https://www.japantimes.co.jp/opinion-2020/08/14/commentary/world-commentary/collective-resilience-way-address-china-challenge>; Victor D. Cha, “Collective Resilience: Deterring China’s Weaponization of Economic Interdependence,” *International Security* 48, no.1 (2023): 91–124; and Victor Cha, “How to Stop Chinese Coercion: The Case for Collective Resilience,” *Foreign Affairs*, January/February 2023.

⁸ White House, “Executive Order on America’s Supply Chains,” Press Release, February 24, 2021, <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains>.

⁹ “U.S.-Japan Competitiveness and Resilience (CoRe) Partnership,” Ministry of Foreign Affairs (Japan), 2021, <https://www.mofa.go.jp/files/100177722.pdf>.

¹⁰ “U.S.-Japan Competitiveness and Resilience (CoRe) Partnership,” White House, Fact Sheet, April 16, 2021, <https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/16/fact-sheet-u-s-japan-competitiveness-and-resilience-core-partnership>.

¹¹ Kyla H. Kitamura, “U.S.-Japan Critical Minerals Agreement,” Congressional Research Service, In Focus, May 20, 2024, <https://crsreports.congress.gov/product/pdf/IF/IF12517>.

of setting up Japan's economic security strategy.¹² Finally, the Kishida administration (October 2021–September 2024) took the last steps in formalizing the Japanese government's policy structure in support of its economic security priorities by drafting and passing the Economic Security Promotion Act (ESPA). Under Prime Minister Kishida, the government also established an economic security minister and upgraded the Economic Security Promotion Headquarters, as well as installing these functions/bureaus within the Foreign and Economic Ministries.

The U.S.-Japan partnership has become the core of the fight to minimize supply chain disruption and deter economic coercion. Capitalizing on the existing FOIP framework and the Quad grouping, the two governments made the issue of supply chain resilience one of the pillars of the first post-pandemic in-person Quad summit in September 2021.¹³ The two governments have also expanded their partnership to other countries from South Korea to Europe. Furthermore, U.S.-Japan collaboration served as a key driver that led to the achievements of the G-7 Hiroshima Summit in May 2023, when the leaders agreed on and announced the “G7 Leaders’ Statement on Economic Resilience and Economic Security.” In its preamble, the leaders “affirm that our cooperation to strengthen economic resilience and economic security will be rooted in maintaining and improving a well-functioning international rules-based system,” and the statement identifies seven priority areas to cover to achieve these goals.¹⁴ On the counter-economic coercion front, G-7 members at the Hiroshima Summit launched the Coordination Platform on Economic Coercion to demonstrate solidarity against such actions (see Togashi’s essay for further discussion).¹⁵

The Future of U.S.-Japan Cooperation in Support of Collective Resilience

U.S.-Japan cooperation on collective resilience has come a long way in a relatively short period in the 2020s. The two countries have profound common interests in boosting economic and technological resilience and supporting the rules-based order. Nonetheless, their ultimate goals and associated concerns are not fully aligned. Especially with the beginning of the second Trump administration, the following three areas will be likely points of discord.

First and most importantly, the U.S. government is unified in its belief that China is the largest source of economic uncertainty and the primary risk to enhancing resilience. Since the first Trump administration, U.S. export control policies have not shied away from explicitly calling for reducing ties with China on national security grounds.¹⁶ Meanwhile, the Japanese government (and many other Asian and European leaders, for that matter) do not identify, at least not explicitly, China as the ultimate or the only perpetrator of supply chain disruption. For Japan, decoupling from China or explicitly targeting it for export controls not only is undesirable but also could be

¹² Liberal Democratic Party, “Teigen: Keizai anzen hosho senryaku sakutei ni mukete” [Proposal: Toward Establishing Economic Security Policies], December 22, 202, <https://www.jimin.jp/news/policy/201021.html>.

¹³ “Joint Statement from Quad Leaders,” White House, September 24, 2021, <https://www.whitehouse.gov/briefing-room/statements-releases/2021/09/24/joint-statement-from-quad-leaders>.

¹⁴ “G7 Hiroshima Summit: Session 5 Economic Resilience and Economic Security,” Ministry of Foreign Affairs (Japan), Overview, May 20, 2023, https://www.mofa.go.jp/ecm/ec/page1e_000686.html.

¹⁵ The G-7 statement further pledges to “use early warning and rapid information sharing, regularly consult each other, collaboratively assess situations, explore coordinated responses, deter and, where appropriate, counter economic coercion, in accordance with our respective legal systems.” See “G7 Leaders’ Statement on Economic Resilience and Economic Security,” White House, May 20, 2023, <https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/20/g7-leaders-statement-on-economic-resilience-and-economic-security>.

¹⁶ “China—Country Commercial Guide,” International Trade Administration, updated April 28, 2023, <https://www.trade.gov/country-commercial-guides/china-us-export-controls>.

economically damaging. Japan's industries are deeply integrated into those in China—a pattern that is repeated across Asian economies. Since the hawkish U.S. stance toward China is unlikely to change between the Biden and Trump administrations, this challenge is likely to continue and even intensify between the United States and Japan.

Second, although collective resilience makes sense to the participating like-minded members to achieve higher stability and economic resilience, a coordinated, policy-driven collective approach is proving very difficult to achieve. The proposed Chip 4 Alliance is a case in point. The U.S. government's attempts to entice the major semiconductor-producing economies of Japan, Taiwan, and South Korea to create an "alliance" with the United States against China in the "chip war" did not fly well with these governments and their businesses.¹⁷ Although the Kishida government agreed in September 2023 to stop exporting advanced chipmaking machines to China, the U.S. intention to cut China totally out of high-end semiconductor markets and not to allow others to do business with it is a difficult sell in Asia, as is the United States' hard security narrative of containment. With the return of President Donald Trump, who is known to be a unilateralist, the collective strategy and cooperation among allies will become even murkier (see Michael Breeman's essay for further discussion).

Third, domestic politics and the protectionist focus of the U.S. economic security strategy also target Japan's economic interest. Although the Biden administration called for stronger collaboration with Japan along with other like-minded countries, it is clear that such calls face limitations. The U.S. government's heightened and tightened export control and investment screening provisions in critical sectors in recent years have carried negative consequences for Japanese business investment in the country. The blocking of Nippon Steel's proposed acquisition of U.S. Steel has demonstrated that domestic political priorities play a key role in this complex relationship, and there is a fine line between economic security for the sake of global economic resilience and for domestic protectionism. With promises of imposing high tariffs on all items coming into the U.S. market, many expect President Trump to implement an "America first" economic policy and intensify protectionism. Furthermore, if the first Trump administration provides any indication as to how the second Trump administration will behave, national security considerations will cast a much larger shadow on U.S. trade and investment policies across the board.

Achieving Resilience in an Era of Disruption: The United States and Japan

The five essays that follow this introduction examine various aspects of economic resilience and the challenges to economic and national security. As the world faces fundamental and rapidly expanding challenges to economic resilience, the United States and Japan, along with other connected economies, have taken measures in response. Although the priorities and strategies vary, the United States and Japan are the principal actors in addressing economic resilience and economic security for the region and the world. The authors highlight the importance of cooperation and coordination in tackling threats and uncertainty by more fully involving both domestic and international players—especially private-sector industrial partners.

¹⁷ Arjun Gargeyas, "The Chip 4 Alliance Might Work on Paper, but Problems Will Persist," *Diplomat*, August 25, 2022, <https://thediplomat.com/2022/08/the-chip4-alliance-might-work-on-paper-but-problems-will-persist>.

In the first essay, Yuichi Hosoya focuses on Japan's recent approach to economic resilience, particularly in the face of economic security challenges. With its history of considering economic security as a part of comprehensive national security, the Japanese government was an early initiator of economic security strategy from the 2010s through now. As a national initiative, the Kishida government prioritized economic security in its National Security Strategy along with the passage and implementation of the ESPA. Meanwhile, the U.S. and Japanese governments have collaborated closely on economic security policies and institutionalized their cooperation through the CoRe Partnership and Economic 2+2. Finally, the Kishida government spearheaded cooperation among like-minded countries toward economic resilience and economic security through the 2023 G-7 Hiroshima Summit. Despite these visible achievements, Hosoya argues that Japan's economic security strategy needs further clarification as the government implements policy measures that tend to be more defensive. Fundamentally, economic security constitutes an integral component of Japan's national security, and the Japanese government will continue to work closely with its partners to enhance the rules-based international order in support of economic resilience.

The second essay by Michael Beeman discusses the U.S. approach, which invokes both national security and economic resilience. The United States, which had long been the guardian and the leader of the postwar rules-based trading system in support of market opening and peaceful interdependence, began to change course in the 2010s in the face of economic security challenges, especially with the rise of Chinese technological and industrial power. As Beeman explains, the United States' pursuit of economic resilience centers on two objectives: protection of leading and critical U.S. technologies, and the bolstering of domestic industrial production and supply chain diversification goals. For the first objective, accelerating protection and development of foundational technologies such as semiconductors and AI has become a critical feature of the U.S. "small yard and high fence" economic security strategy. Meanwhile, new industrial policy and reshoring/friendshoring constitute the core of the production resilience objective. The passage of legislation, coupled with significant fiscal commitments through the CHIPS and Science Act and the Inflation Reduction Act (both passed in 2022), incentivizes domestic production and reshoring of critical items such as semiconductors, solar panels, and EVs with tax incentives and subsidies. Beeman argues, nonetheless, that these policy choices are tied to the United States' domestically driven agendas, and the America-first Trump administration is likely to take even more assertive strategies toward derisking and decoupling in its second term.

In the third essay, Hiroyuki Suzuki shifts the focus of the report to digital infrastructure, digital competition among global companies, and challenges of digital transformation (DX), especially regarding support for the development of digital infrastructure in the global South. Against the backdrop of China's Digital Silk Road under the Belt and Road Initiative, the race in the area of digital technology and connectivity will continue to intensify. Supported by the country's traditional strength in development finance, the Japanese government has worked with its partners to foster resilient digital infrastructure throughout the global South and beyond. One example identified by Suzuki is Japan's collaboration with the United States and Australia in support of stable telecommunication infrastructure in the South Pacific. Moreover, the Japanese government took the lead in launching the G-7 Digital and Technology Ministerial Meeting at the 2023 Hiroshima Summit. The essay concludes by examining three challenging areas for Japan's new digital infrastructure strategy. The first is the geopolitical risks in the Indo-Pacific. As demonstrated by the disruption of undersea cable networks in the South Pacific, the digital infrastructure that sustains

telecommunication, digital, and commercial activities is vulnerable. The second challenge is the convergence of the digital transformation with the green transformation (GX). With the significant electricity needs that data centers demand straining the economies of developing countries in the global South, the fusion of GX and DX is vital. Third, with the rapid development of generative AI, the world faces challenges in establishing digital governance and infrastructure standards. Here, Suzuki argues that both multilateral efforts such as the establishment of Blue Dot Network certification and the engagement of the private sector will be fundamentally important.

As the expansion of the digital economy becomes the global norm, cybersecurity is becoming a major pillar of economic and national security for many countries. In the fourth essay, Mihoko Matsubara discusses how cyberattacks and information operations have become a central part of hybrid warfare, which has intensified since the 2022 outbreak of the war on Ukraine. In addition, China-based Volt Typhoon has launched cyberattacks on U.S. critical infrastructure and attempted to access sensitive data for the last few years. Against Japan, the 2023 ransomware attack on the Port of Nagoya led to the stoppage of the port for two days, resulting in cascading effects and supply chain disruptions. These cyber threats have driven both the U.S. and Japanese governments to strengthen their respective cybersecurity measures. Such efforts are in the front and center of Japan's ESPA, which designates 210 companies across fifteen essential infrastructure service sectors (ranging from electric power to financial institutions to ports) to be managed by multiple layers of regulations against potential risks of disruption. Furthermore, the 2022 National Security Strategy document includes a new mandate for active cyberdefense, including building capabilities to neutralize potential cyberattacks against Japan. On the global level, Japan became a member of the NATO Cooperative Cyber Defence Centre of Excellence and cooperates closely with various entities, including Europol, to tackle the cyber and ransomware challenges. Matsubara identifies that the future steps to address cyber threats require close cooperation with industry partners in the private sector. As such, public-private partnership through a collaborative framework will be needed to enhance cybersecurity resilience.

In the report's final essay, Mariko Togashi focuses on economic security measures to counter economic coercion. The use of coercive measures has increased significantly since the mid-2010s, when China began deploying them to achieve its foreign policy goals. Deterring such economic coercion, whether through denial or punishment, would change the adversary's cost calculation. Japan has opted to resort to a denial-based strategy ever since its economy first encountered such overt coercion by China in the form of a ban on the export of rare earth minerals during a 2010 incident around the Senkaku Islands. By reducing its dependency on China for rare earth minerals, Japan has been able to reduce China's coercive abilities since the incident. Working in cooperation with others to build resilient supply chains for all essential products is a vital aspect of Japan's denial strategy. Along with domestic legislation in support of supply chain resilience (ESPA), Japan has worked to establish multiple forums for countering economic coercion collectively through U.S.-Japan bilateral cooperation (the Economic 2+2); trilateral agreements among the United States, Japan, and South Korea; the Indo-Pacific Economic Framework for Prosperity; and the G-7 coordination platform. Togashi concludes by emphasizing the importance of U.S.-Japan leadership in working with like-minded countries to reduce supply chain vulnerabilities and to collectively tackle economic coercion. Institutionalization of these efforts both domestically and internationally will be essential so that multilateral arrangements persist in the face of changing national leadership.

THE NATIONAL BUREAU *of* ASIAN RESEARCH
NBR SPECIAL REPORT #116 | FEBRUARY 2025

Japan's Approach to Resilience and Economic Security

Yuichi Hosoya

YUICHI HOSOYA is a Professor of International Relations at Keio University. He can be reached at <hosoya@keio.jp>.

EXECUTIVE SUMMARY

This essay argues that Japan's recent approach to resilience and economic security is closely linked to its diplomatic strategy for enhancing the free and open international order based on the rule of law, which has led to renewed U.S.-Japan cooperation.

MAIN ARGUMENT

Amid increased U.S.-China rivalry and Russia's invasion of Ukraine, the impacts of great-power competition on economic interdependence have prompted Japan to pursue economic security through enhancing its self-reliance and technological leadership. Under Prime Minister Fumio Kishida, Japan placed economic security as a top policy priority, with key measures including the appointment of the first minister of state for economic security and the establishment of the Council for the Promotion of Economic Security, which produced the Economic Security Promotion Act. Kishida's advancement of economic security policy built on the 2022 National Security Strategy, which tied the purpose of economic security to ensuring Japan's national security interests. The aforementioned changes in the international environment have also led to renewed U.S.-Japan cooperation, which has prioritized economic security, particularly a de-risking strategy toward China, as a central component of the partnership. This strengthened cooperation has resulted in the U.S.-Japan Competitiveness and Resilience Partnership and the Japan-U.S. Economic Policy Consultative Committee.

POLICY IMPLICATIONS

- Japan's economic security strategy is still ambiguous on several key parts. The Japanese government should pass additional legislation to clarify Japan's definition of economic security and other concrete policy measures.
- More proactive measures should be taken to maximize the impact of Japan's economic security policies, which have traditionally relied on defensive measures.
- The Japanese government should increase cooperation between the government and the private sector, including through additional regulatory steps and direct engagement between government and private-sector stakeholders, in order to strengthen the effectiveness of its economic security strategy.

In his first policy speech at the National Diet in October 2021, Prime Minister Fumio Kishida talked about his vision for Japan's growth. His growth strategy consisted of four pillars, and the third one was "economic security." According to his explanation, under this pillar Japan would seek to advance its efforts to secure strategic goods and materials, prevent outflows of technology, and achieve an autonomous economic structure.¹ Prime Minister Kishida declared that, based on the framework indicated above, "we will build a resilient supply chain and draw up legislative bills that promote Japan's economic security." To attain this goal, he appointed Takayuki Kobayashi, a young and talented Diet member of the ruling Liberal Democratic Party (LDP), as the first minister of state for economic security on October 4, 2021. This made Japan a leader in defining economic security. To implement this vision, Kishida's cabinet established the Council for the Promotion of Economic Security soon after he became prime minister.

In November 2021 the Council for the Promotion of Economic Security held its first meeting and presented three key objectives: "(i) increasing self-reliance, (ii) securing an advantage and indispensability, and (iii) maintaining and strengthening the international order based on basic values and the rule of law."² Within months, it was clear to the expert community that Prime Minister Kishida placed economic security at the center of his policy agenda.³ After seven months of intensive preparation within the Council for the Promotion of Economic Security, with Prime Minister Kishida himself and Economic Security Minister Kobayashi playing key roles, Kishida's cabinet presented the draft Economic Security Promotion Act (ESPA), which was subsequently enacted by the National Diet on May 18, 2022. The purpose of the ESPA is to promote economic security by establishing systems to ensure the stable supply of specified critical products and essential infrastructure services, while also safeguarding designated critical technologies and intellectual property. It also acknowledges the increased complexity of the international geopolitical environment and calls for measures to prevent economic activity that could harm the security of the nation and its citizens.⁴

The ESPA has four important pillars at its core: (1) ensuring resilient supply chains for strategically critical industries, (2) protecting critical infrastructure from disruption, (3) promoting and funding R&D for critical technologies and encouraging public-private cooperation in their development, and (4) establishing a secret program for patents related to national security (the first of its kind in Japan).⁵ The four pillars address both the "promote" side and the "protect" side of Japan's economic security strategy, with the first, second, and fourth pillars relating mainly to the former, while the third pillar relates primarily to the latter.⁶

In sum, this legislation seeks to strengthen Japan's ability to combat economic coercion by enhancing its "strategic autonomy" and pursuing "strategic indispensability." One aspect of this vision is to continue developing and advancing key Japanese technologies on which countries and

¹ "Policy Speech by Prime Minister Kishida Fumio to the 205th Session of the Diet," Prime Minister's Office of Japan, October 8, 2021, https://japan.kantei.go.jp/100_kishida/statement/202110/_00005.html.

² Ministry of Economy, Trade and Industry (Japan), *White Paper on International Economy and Trade 2023* (Tokyo, 2023), 205, <https://www.meti.go.jp/english/report/data/wp2023/pdf/2-1-2.pdf>.

³ Kazuto Suzuki, "Inching Toward Economic Security: Kishida Cabinet to Focus on Defensive Tools," Nippon.com, February 9, 2022, <https://www.nippon.com/en/in-depth/a07901>.

⁴ A translation of the ESPA is available at <https://www.japaneselawtranslation.go.jp/en/laws/view/4523/en>.

⁵ Cabinet Office (Japan), "Outline of the Economic Security Promoting Act," trans. Japanese Law Translation, <https://www.japaneselawtranslation.go.jp/outline/75/905R403.pdf>. For further discussion of the Japanese government's efforts to promote resilient critical infrastructure through improved cybersecurity, see Mihoko Matsubara's essay in this report.

⁶ Ministry of Economy, Trade and Industry (Japan), *White Paper on International Economy and Trade 2023*.

industries around the world depend.⁷ “Strategic autonomy” and “strategic indispensability” are generally regarded as the two key concepts that describe the features of Japan’s economic security strategy. On the one hand, “strategic autonomy” means strengthening the foundations necessary to maintain Japan’s social and economic activities while avoiding excessive dependence on other countries.⁸ On the other hand, “strategic indispensability” means maintaining, strengthening, and expanding the areas where Japan is considered irreplaceable by the international community.⁹ Japan must defend its own national interests based on these two concepts at a time when economic security is becoming one of the core issues of great-power competition.

Many experts have noted that Japan was a first mover among major advanced economies to draft and implement economic security legislation.¹⁰ Mireya Solís, for example, has argued that “the deterioration of Sino-American relations, the growing weaponization of economic interdependence, and production dislocation amid the pandemic have given rise to a new track of economic security.”¹¹ From this perspective, the enactment of the ESPA is Japan’s response to the expansion of U.S.-China strategic competition.

However, economic statecraft has always been at the center of postwar Japan’s foreign policy.¹² Given the constraints on military activity mandated by Article 9 of the country’s constitution, it has been necessary for Japan as a pacifist power to rely mainly on economic measures in pursuing its national interest. This economic-focused approach to foreign policy and grand strategy is often called the Yoshida Doctrine, after Prime Minister Shigeru Yoshida, who first proposed an economic-focused approach to international diplomacy as early as 1950. Yoichi Funabashi, a leading Japanese journalist, wrote a book entitled *Keizai anzenhoshō ron* (On Economic Security) in 1978, reflecting the concept’s early emergence into widespread policy consciousness in Japan. Since the beginning of the country’s economic rise, spurred on by effective industrial and technology policy in the middle of the 1970s, Japan has often been regarded as a frontrunner of economic security policy.

While economic security has been a familiar concept for Japanese policymakers over multiple decades, the governments of both Kishida and his predecessor, Prime Minister Yoshihide Suga, accelerated steps to develop the modern formulation of Japan’s economic security strategies. This essay argues that Japan’s recent approach to resilience and economic security is closely linked to its diplomatic strategy for enhancing the free and open international order based on the rule of law.

Economic Security in Japan’s National Security Strategy

Even beyond the ESPA, economic security was at the center of Kishida’s policy agenda during his premiership. In December 2022, his cabinet adopted the new National Security Strategy, which emphasized the importance of economic security in a way not seen in previous strategies. It provides

⁷ Kazuto Suzuki, “How Will the Economic Security Law Change Japan’s Sci-Tech Policy?” Tokyo Foundation for Policy Research, May 9, 2023, <https://www.tokyofoundation.org/research/detail.php?id=943>.

⁸ Kazuto Suzuki, “Japan’s Economic Security and Semiconductor Industry,” Japan Institute of International Affairs, AJISS-Commentary, no. 293, February 3, 2022, https://www.jiia.or.jp/en/ajiss_commentary/japans-economic-security-and-semiconductor-industry.html.

⁹ Ibid.

¹⁰ “Japan’s Economic Security Legislation,” European Parliamentary Research Service, July 2023, [https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/751417/EPRS_ATA\(2023\)751417_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/751417/EPRS_ATA(2023)751417_EN.pdf).

¹¹ Mireya Solís, *Japan’s Quiet Leadership: Reshaping the Indo-Pacific* (Washington, D.C.: Brookings Institution Press, 2023), 143.

¹² Yuichi Hosoya, “Kokka senryaku to shite no Keizai azenhoshō” [Economic Security as National Strategy], in *Keizai anzenhoshō to wa nanika?* [What Is Economic Security?], ed. Institute of Geoeconomics (Tokyo: Toyo Keizai, 2024), 41–42.

a clear definition of the concept, stating that “economic security is to ensure Japan’s national interests, such as peace, security, and economic prosperity, by carrying out economic measures.”¹³

This National Security Strategy is the second after Prime Minister Shinzo Abe initiated the introduction of Japan’s first National Security Strategy in 2013. At that time, economic security was not at the center of Japan’s national security debates. In April 2020, however, the Japanese government added an economic division to the National Security Secretariat. In July 2020 the government included the term “economic security” for the first time in its policy guideline, titled “Basic Policy of Economic and Financial Management and Reform 2020.” The rising tensions between the United States and China during the first Trump administration were the backdrop against which Japan began to focus on economic security. It was therefore natural that economic security was included in Japan’s 2022 National Security Strategy document.

As the strategy was being drafted, Russia’s invasion of Ukraine was seriously damaging the foundation of the rules-based international order. Therefore, the strategy also clearly tied the risk of economic disruption to Japan’s core security interests, stating that “in the face of various threats at hand through economic means, Japan will coordinate ideas on necessary economic measures and execute these measures comprehensively, effectively and intensively to enhance Japan’s self-reliance and to secure the advantage and indispensability concerning our technologies and others.”¹⁴ Recognizing these threats, the strategy clearly affirms the objectives of self-reliance and technological leadership that motivated the passage of the ESPA earlier that same year, indicating that the objectives of the law are central to the country’s overall strategy.

Thus, the 2022 National Security Strategy incorporated economic security into the Kishida administration’s core policy document, reflecting the importance placed on this topic since the beginning of the administration.¹⁵ The National Security Secretariat began to stress technological capabilities as one of five components of “comprehensive national power,” which also includes diplomatic capabilities, defense capabilities, economic capabilities, and intelligence capabilities. The Kishida administration aimed to enhance Japan’s technological capabilities to increase national power, moving beyond mere discussions of economic diplomacy to identify economic security as an integral part of Japan’s national security strategy for the first time.

The U.S.-Japan CoRe Partnership and the Economic 2+2

The foundation of Japan’s economic security policy had already been designed by the cabinets of Shinzo Abe and Yoshihide Suga, building off their diplomatic strategy for consolidating the rules-based international order in the context of rising U.S.-China confrontation and Russia’s invasion of Ukraine. The Japanese government has repeatedly described these developments as striking at the foundation of this order. To navigate U.S.-China rivalry, policies of de-risking and friendshoring have emerged globally, which are leading to supply chain shifts and increased cooperation and coordination among like-minded countries.¹⁶

¹³ Cabinet Office (Japan), *National Security Strategy of Japan* (Tokyo, December 2022), <https://www.cas.go.jp/jp/siryou/221216anzenhoshou/nss-e.pdf>.

¹⁴ Ibid.

¹⁵ Yoshiyuki Sagara, “Japan Integrated Economic Security into Its New National Security Strategy,” Institute of Geoeconomics, December 22, 2022, <https://instituteofgeoeconomics.org/en/research/2022122642919>.

¹⁶ Tsuyoshi Kawase, “The Future of a World Divided into Economic Blocs: Multilateral Trade Contributes to Economic Security,” Discuss Japan: Japan Foreign Policy Forum, June 12, 2023, <https://www.japanpolicyforum.jp/economy/pt2023061211402313110.html>.

While Japan's economic security strategy has long been connected to its vision for global order, these changes taking place within the international system have renewed U.S.-Japan cooperation, with the concept of economic security as a core driving factor.¹⁷ The shared emphasis by the U.S. and Japanese governments on resilience has made the bilateral partnership increasingly relevant. Prime Minister Suga fully recognized this trend and pursued a stronger partnership with the United States to support Japan's economic security priorities. In an international environment where the U.S.-China rivalry has continued to affect other Indo-Pacific regional players, Japan felt a strategic imperative to enhance the Japan-U.S. alliance. In particular, Prime Minister Suga aimed to align with the United States' decoupling or de-risking strategy toward China. With the global supply chain undergoing a significant realignment, it was necessary to coordinate policies relating to resilience and economic security.

When Prime Minister Suga visited Washington, D.C., on April 16, 2021, to meet President Joe Biden, according to the official readout of the meeting, the two leaders "noted their shared universal values, including freedom, democracy, human rights, and the rule of law, and they shared the view on strengthening the Japan-U.S. Alliance, which is the cornerstone of peace and prosperity in the Indo-Pacific region."¹⁸ More tangibly, they agreed to establish the U.S.-Japan Competitiveness and Resilience (CoRe) Partnership.¹⁹ This partnership is an important step forward to make the bilateral relationship more relevant in the field of economic security based on the building and strengthening of supply chains among like-minded countries.

The statement announcing the formation of the CoRe Partnership emphasized that the "new partnership for competitiveness and innovation carries on [the] tradition [of bilateral cooperation], focusing on scientific and technological advances." It highlights a number of specific technological priorities, including biotechnology, artificial intelligence, quantum information science and technology, civil space cooperation (including the Artemis program and asteroid exploration), and secure information and communications technology, among others.²⁰ While both the Japanese and U.S. media focused on the issue of the Taiwan contingency at this summit, the agreement to promote the CoRe Partnership was more significant in terms of the tangible impact on resilience in the bilateral relationship. The CoRe Partnership also aims to enhance cooperation in the fields of the digital economy, the Open Radio Access Network, cybersecurity and critical infrastructure resilience, science and technology, civil space, international standards, export controls, and supply chain resilience, among others.²¹ As a result, U.S.-Japan cooperation has expanded to include these new policy areas, reflecting both countries' heightened interest in economic and technological resilience.

In an attempt to institutionalize the collaboration promised by the CoRe Partnership, the U.S. and Japanese governments established a new framework for consultation in the field of economic security. On July 29, 2022, the first meeting of the Japan-U.S. Economic Policy Consultative

¹⁷ Shihoko Goto and Lucas Myers, "Testing the Bond of Shared Economic Security Interests," in "Reshaping U.S.-Japan Economic Security Partnership in the Indo-Pacific," Wilson Center, 2023, <https://www.wilsoncenter.org/publication/reshaping-us-japan-economic-security-partnership-indo-pacific>.

¹⁸ "Japan-U.S. Summit Meeting," Ministry of Foreign Affairs (Japan), April 16, 2021, https://www.mofa.go.jp/page4e_001123.html.

¹⁹ "U.S.-Japan Competitiveness and Resilience (CoRe) Partnership," Ministry of Foreign Affairs (Japan), April 16, 2021, <https://www.mofa.go.jp/files/100177722.pdf>.

²⁰ Ibid.

²¹ "The U.S.-Japan Competitiveness and Resilience (CoRe) Partnership," Ministry of Foreign Affairs (Japan), Fact Sheet, May 23, 2022, <https://www.mofa.go.jp/mofaj/files/100347255.pdf>.

Committee (the Economic “2+2”) was held in Washington, D.C.²² The meeting was attended by Minister for Foreign Affairs Yoshimasa Hayashi and Minister of Economy, Trade and Industry Koichi Hagiuda, as well as Secretary of State Antony Blinken and Secretary of Commerce Gina Raimondo. Foreign Minister Hayashi stated that “the Economic 2+2, in which diplomacy, security, and the economy are discussed as one, is a framework that responds to the demands of our time, and that Japan and the United States intend to exercise leadership to maintain and strengthen the free and open rules-based international economic order as well as sustainable and inclusive economic growth.”²³ Reflecting the Japanese government’s priorities, Foreign Minister Hayashi clearly linked the issue of economic security with the “strengthening of the free and open rules-based international economic order.” Moreover, the fact that economic issues were given equal billing at a bilateral summit reflects the growing importance to the partnership of economic diplomacy, which has long been central to Japan’s economic security strategy.

At this Economic 2+2, the ministers discussed four topics: (1) realizing peace and prosperity through the rules-based economic order, (2) countering economic coercion and unfair and opaque lending practices, (3) promoting and securing critical and emerging technologies and critical infrastructure, and (4) strengthening supply chain resilience. On the first topic, Foreign Minister Hayashi emphasized “the importance of Japan and the U.S. working together with like-minded countries to maintain and develop the international order as well as to ensure the economic security of each country, given the strong influence of economic matters on diplomacy and security today.”²⁴ At the end of the discussion, the four ministers “reaffirmed the need for Japan and the U.S. to remain the greatest advocates of a free and open rules-based international economic order.” They also “reaffirmed their determination to lead international cooperation in areas such as economic policy of both countries, the establishment of a regional economic order...and economic security.”²⁵ As China has resorted to economic coercion and the so-called weaponization of economic interdependence (discussed at length in Mariko Togashi’s essay for this report), both the U.S. and Japanese governments have begun to reorient their foreign economic policies. China’s closer cooperation with Russia has further sharpened the United States’ and Japan’s perception of the limits of their cooperation with China. Thus, the start of the Economic 2+2 marked an important turning point for their perception of the need for decoupling or de-risking with respect to China.

The joint statement from the Economic 2+2 highlighted that cooperation between the two countries is essential to achieve the objectives presented in the CoRe Partnership. It also emphasized collaborating with like-minded partners and jointly working to strengthen the rules-based economic order in the Indo-Pacific region and beyond.²⁶ Thus, the CoRe Partnership has become a solid foundation establishing shared principles around economic resilience to inform deeper cooperation in support of the rules-based economic order at a time when Russia’s invasion of Ukraine poses a serious threat to international peace and stability.

²² “Japan-U.S. Economic Policy Consultative Committee Meeting (the Economic ‘2+2’),” Ministry of Foreign Affairs (Japan), July 29, 2022, https://www.mofa.go.jp/na/na2/us/page6e_000296.html.

²³ Ibid.

²⁴ Ibid.

²⁵ Ibid.

²⁶ “Joint Statement of the U.S.-Japan Economic Policy Consultative Committee Strengthening Economic Security and the Rules-Based Order,” Ministry of Foreign Affairs (Japan), July 29, 2022, <https://www.mofa.go.jp/files/100376270.pdf>.

The second ministerial meeting of the Economic 2+2 was held on November 14, 2023. Yoko Kamikawa joined the meeting as foreign minister, and Yasutoshi Nishimura joined as minister for the Ministry of Economy, Trade and Industry. At the outset, Foreign Minister Kamikawa pointed out that while the international community is facing many challenges, such as the prolonged Russian invasion of Ukraine, unstable and vulnerable supply chains, the global energy and food crisis, and the ongoing conflict between Israel and Palestine, steady progress was being made in cooperation between Japan and the United States as well as among like-minded countries.²⁷

The meeting focused on two topics: strengthening the rules-based economic order in the Indo-Pacific region, and strengthening economic resilience, including through the promotion and protection of critical and emerging technologies.²⁸ On the first topic, the U.S. and Japanese governments agreed to strengthen the rules-based economic order in the Indo-Pacific region by cooperating in seven areas: (1) promoting economic engagement with the Indo-Pacific, (2) addressing nonmarket policies and practices, (3) addressing economic coercion, (4) addressing trade restrictions not based on scientific principles or substantiated by scientific evidence, (5) building transparent, resilient, and sustainable supply chains, (6) promoting quality infrastructure and sustainable investment and addressing opaque lending practices, and (7) protecting personal data and privacy.²⁹ Both the United States and Japan became increasingly interested in deepening their cooperation in the areas of economic security and critical and emerging technologies. As it appeared more difficult than before to reach a compromise in either the World Trade Organization or the G-20, cooperation among like-minded partners in these areas became essential.

In 2023, Japan held the presidency of the G-7, while the United States hosted the Asia-Pacific Economic Cooperation (APEC) Summit. Seizing on the opportunities presented by their leadership roles in key multilateral forums, the two governments affirmed their “continued commitment to enhancing the rules-based international economic order and making our economies more competitive and resilient.”³⁰ Like the U.S.-Japan Security Consultative Committee (known as the Security “2+2”), which was established in 2000, the Economic 2+2 has become an important tool for the U.S.-Japan partnership in the field of economic security.

The G-7 Hiroshima Summit and Economic Security

The G-7 summit in Hiroshima held on May 19–21, 2023, marked an important step forward for the advancement of cooperation among like-minded countries in the field of economic resilience and economic security. In the communique released at the summit, the G-7 leaders agreed to take concrete steps to “coordinate our approach to economic resilience and economic security that is based on diversifying and deepening partnerships and de-risking, not de-coupling.”³¹ In the section “Economic Resilience and Economic Security,” they stated that “ensuring economic resilience and economic security globally remains our best protection against the weaponization

²⁷ “Second Ministerial Meeting of the Japan-U.S. Economic Policy Consultative Committee (the Economic ‘2+2’),” Ministry of Foreign Affairs (Japan), November 14, 2023, https://www.mofa.go.jp/na/na2/us/page4e_001514.html.

²⁸ Ibid.

²⁹ “Joint Statement of the Japan-U.S. Economic Policy Consultative Committee,” Ministry of Foreign Affairs (Japan), November 14, 2023, <https://www.mofa.go.jp/files/100581690.pdf>.

³⁰ Ibid.

³¹ “G7 Hiroshima Leaders’ Communique,” Ministry of Foreign Affairs (Japan), May 20, 2023, <https://www.mofa.go.jp/files/100506878.pdf>.

of economic vulnerabilities.”³² Amid the ongoing Russia-Ukraine conflict and increased Chinese economic coercion, the G-7 provided a foundation for cooperation among the like-minded liberal democracies. Japan’s leadership of the summit in 2023 represented the strongest use to date of this platform to pursue shared objectives around economic resilience. Participants also pledged to “advance economic policies that enhance global economic resilience and economic security to protect against systemic vulnerabilities” and to engage in dialogue and cooperation—both within the G-7 and with partners around the world, including developing countries.³³

Session 5 of the G-7 Hiroshima Summit was devoted to economic resilience and economic security. In the beginning of this session, Prime Minister Kishida stated that economic security was included in the summit agenda for the first time due to the increased importance of responding effectively and in a coordinated manner to economic security challenges.³⁴ The G-7 leaders affirmed that the group will be united in enhancing the resilience of supply chains and critical infrastructure, strengthening a joint response to nonmarket policies and practices (as well as to economic coercion), and appropriately managing critical and emerging technologies.

Recognizing that economic security is a strategic challenge that the G-7 should tackle, the leaders pledged to closely coordinate in a holistic manner through the G-7 framework.³⁵ They also agreed to “enhance collaboration by launching the Coordination Platform on Economic Coercion to increase our collective assessment, preparedness, deterrence and response to economic coercion, and further promote cooperation with partners beyond the G-7.”³⁶ As China’s influence extends into global supply chains, the G-7 countries are increasingly vulnerable to Chinese economic coercion. Therefore, it is a logical decision for them to exhibit solidarity in their approach to economic security and resilience.

Just as the Economic 2+2 has worked to institutionalize the principles of the U.S.-Japan CoRe Partnership in a bilateral context, the G-7 upgraded its effort to coordinate policies by establishing the Coordination Platform on Economic Coercion. Indeed, it is easy to see this platform as being directly influenced by the progress of the Economic 2+2 in achieving tangible results during the previous year, as was discussed above. The specific ways in which the platform will address these challenges are discussed in detail in Togashi’s essay for this report.

The Way Ahead

This essay has shown how Japan has been a leading promoter of economic security among major powers, both through its national legislation and strategy and through its bilateral and multilateral leadership. However, the country’s economic security strategy includes many ambiguous parts, and further clarification of concrete policy measures is needed. For example, there is still no unified definition of economic security contained in the ESPA, which recognizes four pillars. In addition, the National Diet enacted a new security clearance system in May 2024. Thus, additional

³² “G7 Hiroshima Leaders’ Communique.”

³³ Ibid.

³⁴ “G7 Hiroshima Summit (Session 5 Economic Resilience and Economic Security),” Ministry of Foreign Affairs (Japan), May 20, 2023, https://www.mofa.go.jp/ecm/ec/page1e_000686.html.

³⁵ Ibid.

³⁶ “G7 Hiroshima Leaders’ Communique.”

legislation will be needed to ensure a more effective, coordinated economic security policy for Japan.

At the same time, rooted in a postwar tradition of pacifism, Japan's approach to economic security relies mainly on defensive measures. To maximize the impact of its economic security policy, however, Japan will need to adopt more proactive measures. In addition, an effective economic security policy depends on cooperation between the government and the private sector, which will require additional regulatory steps and direct engagement between the government and private stakeholders.

Facing multiple challenges, Japan has taken a strategic approach to resilience and economic security. While pursuing economic security as an integral part of national security, it has also tried to enhance the rules-based international order. At the same time, Japan needs like-minded partners to pursue this path. Its current prime minister, Shigeru Ishiba, has pledged to base his foreign policy on Kishida's policy trajectories. While his political capital is expected to be limited, continuity in the general trends identified in this essay will likely be the order of the day.

The United States' New Search for Economic Resilience

Michael Beeman

MICHAEL BEEMAN is a former Lecturer in international policy and Visiting Scholar at Stanford University's Walter H. Shorenstein Asia-Pacific Research Center and is the former Assistant U.S. Trade Representative for Japan, Korea, and APEC. He can be reached at <profmbeeman@gmail.com>.

EXECUTIVE SUMMARY

This essay argues that the redefinition and expansion of traditional security-focused objectives by Washington is resetting the role of the state in the economy and leading policymakers to broadly reset U.S. international commitments in the name of economic resilience, with dramatic implications for the rules-based international economic order.

MAIN ARGUMENT

The U.S.'s pursuit of economic resilience is transcending its traditional, narrowly defined goal of protecting critical U.S. technologies with sweeping new efforts to protect against a more extensive array of perceived external risks to U.S. economic security. From countering cyberattacks to mitigating climate change to reducing dependencies on exports from countries of concern, policymakers are reassessing the nation's exposure to these and other vulnerabilities and instituting new economic tools to respond to them. Bolstering economic resilience—a new zeitgeist reflecting these broader economic security aims—has led to reinvigorated steps to redirect an array of more traditional trade and investment decisions in industries such as electric vehicles and solar panels toward new national economic goals. These measures range from expanding and strengthening technology controls for U.S. exports and foreign investments in areas such as advanced semiconductors and artificial intelligence to the introduction of new incentives such as industrial subsidies and tariff increases. These choices weaken the adherence of the U.S. to the rules and principles of open and liberal trade that it once promoted and pose new challenges both for its foreign relations, including with allies such as Japan, and for domestic and foreign businesses operating in the U.S. and around the world.

POLICY IMPLICATIONS

- Washington's newly expanding definition of economic security is redefining priority U.S. national interests. Driven by domestic political change and new technological and global realities, this fundamental reorientation is transforming U.S. policy choices toward trade rules, fiscal priorities, and technological controls and incentives in the pursuit of economic resilience.
- New U.S. policy choices are eroding U.S. support for the rules-based approach to global trade and economic relations that Washington long championed, with major impacts on the future of the international trading system.
- From allies and adversaries to U.S. and foreign businesses, these choices are having a profound impact on the stability and security of the global international system that defined the past several decades.

When viewed from abroad, the United States' indigenous capacity for economic resilience appears immense. Its outsized wealth and natural resources, capacity for technology and innovation, flagship research universities, and vigorous entrepreneurialism, as well as the U.S. dollar's position as the world's reserve currency, are just a few of the attributes that have enabled the country to maintain its position as the world's largest and, arguably, most dynamic and diverse economy. It is striking, therefore, that an American zeitgeist of concern over economic dependence on foreign goods, production, and technologies has re-emerged in recent years, elevating economic "resilience" as a new national policy imperative. As Washington's decision-makers rush to reassess and reduce the United States' vulnerability to a range of potential foreign supply or other dependency shocks, they are implementing new measures to "de-risk" the U.S. economy by disentangling and diversifying the nation's dependency on foreign production and sources of critical goods. These steps have seen mixed success. They also are having outsized impacts on U.S. adversaries and allies alike, raising new diplomatic challenges and carrying large implications for the United States' commercial and technological leadership in new industries such as artificial intelligence (AI).

This essay begins with a short review of past priorities and policies. It then summarizes the various threads and motives underlying the United States' push for economic resilience and the steps Washington is taking to implement new policies to secure its own technological and industrial future. These actions are changing the nature of its economic and commercial relationships, including with allied countries like Japan. Some of the larger implications of these efforts for the United States' future international engagements are also explored.

The Evolution of the U.S. National Security State

Motivated by the strategic imperative to defend itself and the free world, the United States developed during the Cold War a new national security apparatus that, over time, increasingly included security-focused policies with economic components. Several of these policies remain in place today. They include the Committee on Foreign Investment in the United States (CFIUS) system to review and, if necessary, limit foreign direct investment in the United States, along with an extensive legal and regulatory export control regime to systematically monitor and restrict exports of sensitive products and technologies with significant national security implications. These systems serve national security as their primary objective, although certain concerns focused on economic security also have proved to be influential in turning away foreign commercial investment in limited cases.¹

Through the Cold War and into the 1990s and early 2000s, as Washington limited access to a narrow range of critical technologies and products for national security, it simultaneously pursued a policy of open international trade and investment in goods and services. The United States helped establish and then lead the postwar rules-based trading system, based on principles of nondiscrimination and gradual market opening, to foster stable, predictable, and open global trade. It did so for its own growth and commercial objectives, as well as to help prevent the world from returning to pre-World War II beggar-thy-neighbor trade policies that inflamed

¹ See, for example, the case of more informal U.S. political pressure that contributed to a planned takeover of a U.S. semiconductor manufacturer to be scrapped. David E. Sanger, "Japanese Purchase of Chip Maker Canceled after Objections in U.S.," *New York Times*, March 17, 1987.

international tensions. For 75 years following the end of global war in 1945, international trade soared under this system as nearly every nation eventually became a member. Rules-based trade served a range of economic security goals that recognized the benefits of peaceful interdependence to support global growth and poverty alleviation through generally predictable opportunities for nations to trade.

Accordingly, except for its restrictions on a narrow range of military-use technologies and goods, Washington adopted a generally open international posture toward economic and commercial activity. Maintaining this open approach sparked domestic political controversy at times, especially when foreign governments and industries organized to capitalize on it to supercharge their own export and development goals. During the 1980s, challenges posed by Japan's targeted policies to promote specific commercial technologies and industrial sectors contributed to the United States' first national reckoning with this open approach, leading policymakers to respond to what a special MIT commission described as "a decline in U.S. industrial performance perceived to be so serious as to threaten the nation's economic future."²

A generation later, China's technological and industrial targeting and other policies, along with its re-emergence as a strategic adversary, triggered the start of a second reckoning, ushering in another national imperative to de-risk U.S. entanglements with China and other countries to bolster U.S. economic security. The method and impact of China's industrial and technological rise have led to even greater challenges than those posed by Japan decades earlier. From the mid-2010s into the 2020s, the United States' renewed prioritization of economic security included both a deepening and building out of traditional military-focused technology control efforts alongside a broad new expansion of industrial self-reliance and other objectives pursued under the umbrella term of "economic resilience." The Obama administration, for example, cited resilience as a motivation to tackle climate-related challenges alongside emerging new technological vulnerabilities such as cybersecurity.³ Beginning in 2017, the Trump administration took a sharper turn to redefine, widen, and elevate U.S. economic security aims. Paramount among its priorities was to spurn the United States' core commitment to the open global trading system in favor of new tariffs and other policies that prioritized industrial self-reliance and sovereignty in the pursuit of an "America first" brand of economic security. Following the revelation of supply chain vulnerabilities that resulted in global supply shocks for some essential goods during the Covid-19 pandemic, the Biden administration took a less confrontational but not dissimilar approach by invoking "resilience" and "de-risking" as reasons to maintain tariffs and build out efforts to increase U.S. industrial and technological self-reliance. The remainder of this essay focuses on these most recent efforts and developments.

The United States' Pursuit of Economic Resilience

Today, the United States' pursuit of economic resilience is focused on two broad objectives. The first is the substantial deepening of efforts to protect leading and critical U.S. technologies, both to limit their availability for military and other national security applications by U.S. adversaries

² Michael L. Dertouzos, Robert M. Solow, and Richard K. Lester, *Made in America: Regaining the Productive Edge* (Cambridge: MIT Press, 1989), ix.

³ The Obama administration referenced the need for "resilience" when formulating new policies to secure critical infrastructure and to address climate change. See, for example, White House, "Critical Infrastructure Security and Resilience," Presidential Policy Directive, February 12, 2013; and White House, "Preparing the United States for the Impacts of Climate Change," Executive Order 13653, November 1, 2013.

and to protect the U.S. technological edge in foundational technologies. These steps include extending and expanding traditional U.S. national security state goals and tools to cover a wider range of technologies in industries, sectors, and products subject to these controls. The second is to bolster domestic industrial production and supply chain diversification goals. Individual measures range widely, but they generally focus on either re-establishing or expanding industrial capacity at home in designated sectors or reducing in other ways foreign supply chain risks and vulnerabilities. The following subsections examine the new goals shaping economic resilience in each of these dimensions.

Re-tooling the National Security State for Economic Resilience

The Biden administration characterized its policy as a “small yard, high fence” approach to securing the United States’ technological resilience.⁴ This branding, however, reflects little new or revolutionary in U.S. declaratory policy around export controls. Washington’s preexisting controls on exports, inward investment restrictions, and other policies over several decades have been used to achieve a similar end—protecting (“high fence”) a narrow (“small yard”) set of technologies essential for national security. Alongside this approach, U.S. policy has prioritized placing few such limitations on businesses and individuals for ordinary commercial activity. Since the late 2010s, however, U.S. administrations have pursued a broad expansion in these restrictions, principally in response to concerns with China’s rapidly developing technological prowess and its implications for U.S. technological leadership.

The shift in the U.S. approach to enhance technological resilience has been to build this “high fence” a little taller and to make its “small yard” ever larger through adding more goods to the list of potentially sensitive technologies. Characteristic of these efforts are the Trump administration’s bans not only on the use in the United States of telecommunications technology (e.g., switching equipment) made or sold by foreign companies of concern but on the export of U.S. inputs to these firms. These steps to reduce the United States’ technological vulnerability to Chinese entities in the commercial telecommunications sector soon after were emulated by several other governments.

Washington’s urgency to erect defenses against real and potential threats from China helped drive a bipartisan consensus to enact new legal tools to defend against them, a remarkable feat given deep U.S. political division on other issues during the same period. These new tools are contained in two sweeping overhauls passed by the U.S. Congress in 2018—one to comprehensively update and reform the United States’ export control regime (the Export Control Reform Act) and the other to overhaul its system of foreign investment reviews and protections (the Foreign Investment Risk Review Modernization Act).⁵ Among other steps, both laws placed a higher priority on mitigating the risks of sensitive technologies and called for the executive branch to examine and implement controls on a broader array of dual-use goods (commercial products with technologies that have potential defense or other national security implications). While many of these reforms are not limited to specific countries, each new toolkit has been customized to better facilitate its use vis-à-vis Chinese entities. Thus, China has impelled U.S. administrations to take bolder and broader actions to strengthen the United States’ technological resilience.

⁴ “Remarks by National Security Advisor Jake Sullivan on the Biden-Harris Administration’s National Security Strategy,” White House, October 12, 2022.

⁵ For comprehensive overviews of these legislative reforms, see “The U.S. Export Control System and the Export Control Act of 2018,” Congressional Research Service, CRS Report for Congress, R46814, June 7, 2021; and “Foreign Investment Risk Review Modernization Act (FIRRMA),” Congressional Research Service, CRS Insight, IN10924, July 3, 2018.

The Biden administration took additional steps in the early 2020s to newly define and safeguard other technological risks. These include developing new regulations to ban the sale or sharing of sensitive data on U.S. citizens with designated countries, as well as new inquiries to examine the necessity of further controls on the collection and control of other U.S. data in commercial products and services of Chinese-owned or -controlled entities (whether interconnected autonomous driving systems or remote monitoring and control of electronic operating systems in cranes at U.S. ports).⁶

At the epicenter of the U.S. search for technological resilience is the semiconductor industry. Long treated as primarily a commercial sector, the United States' new concerns about dual-use technologies and economic competitiveness have revealed vulnerabilities up and down the production process and across supply chains, especially for advanced chips, leading to a wave of new "higher" fence, "larger" yard policy responses from Washington. Decisions in this sector epitomize the new challenges, issues, and concerns for regulators and commercial actors alike.

Already a growing economic security concern by the late 2010s, the interruption of production and resulting shortages of semiconductors during the Covid-19 pandemic contributed to a cascade of major supply chain bottlenecks across consumer goods and other industries and exposed deep vulnerabilities in global supply chains. Chip shortages also underscored the United States' high dependence on foreign supply. Set against China's rising use of economic coercion (the weaponization of curbs on imports or exports to achieve political goals), along with deepening concerns over China's intentions vis-à-vis Taiwan (home to the most advanced chip production in the world), the need to bolster U.S. economic security and resilience in the chip sector took on a particular new urgency.

To slow Beijing's strides toward attaining advanced chipmaking capacity, the United States took the major step in October 2022 of banning exports to China of the highest-end chips as well as semiconductor-manufacturing machines by the sole U.S.-based maker. To avoid disadvantaging this U.S. firm and to slow China's capacities, Washington sought pledges from the two other nations with these capabilities—the Netherlands and Japan—to also ban their firms from exporting the most advanced chipmaking machines to China. While they agreed to keep their companies from selling to and pursuing other commercial opportunities in China, the boundaries of cooperation were still tested over issues such as whether to prohibit these companies from also servicing their machines in operation in China's chip factories.

China is countering by working to circumvent these restrictions and obtain the most advanced chips and their underpinning technologies. It also has increased state subsidies to move its indigenous industry into the world's most advanced chipmaking club. These are just a few of the challenges the United States faces in its attempt to limit exports and technological know-how amid a new range of competing commercial and economic security goals. As U.S. policymakers peel back and examine each layer of the threat in the attempts to circumvent existing U.S. policy measures targeting established industries such as semiconductors, they are discovering further potential vulnerabilities that call for deeper inquiry and possible action. Among these new concerns is the risk of technology leakage through some outward investments by U.S. entities

⁶ "President Biden Issues Executive Order to Protect Americans' Sensitive Personal Data," White House, Fact Sheet, February 28, 2024; "Citing National Security Concerns, Biden-Harris Administration Announces Inquiry into Connected Vehicles," U.S. Department of Commerce, Press Release, February 29, 2024; and "Biden-Harris Administration Announces Initiative to Bolster Cybersecurity of U.S. Ports," White House, Fact Sheet, February 21, 2024.

into foreign countries, along with new consideration of reasons to disallow transactions that may undermine U.S. economic security.

How to implement such a system in a way that does not unfairly disadvantage U.S. businesses vis-à-vis their foreign competitors, but that targets only necessary restrictions on their activities, is just one challenge underpinning many of these new U.S. approaches. New restrictions announced on U.S. outbound investment in Chinese companies in limited product and service areas raise similar issues of whether further national security requirements will limit the ability of U.S. firms to invest in China and thereby unproductively hinder the expansion of their operations to stay ahead in competition with Chinese and other foreign firms.⁷

Another new U.S. resilience priority is to better protect “foundational” commercial technologies in leading-edge sectors, including prior to their widespread commercialization. One example is the effort underway to limit foreign access to quantum-computing components and know-how—a technology not yet commercialized but with seismic potential in its commercial and defense applications. For AI and other new foundational technologies already on the market, regulators are left making decisions in real time to balance the need to give U.S. firms room to grow their businesses with new technology-related controls that constrain some potential sales and exports. Attempts to keep AI capabilities out of the hands of adversaries and their militaries serve national security goals, but if they employ restrictions too onerous for U.S. companies to maintain their commercial and technological lead, these restrictions ultimately could undermine the United States’ economic security over the longer term.

To date, Washington’s AI-related controls have been placed on exports of underpinning technologies, principally the leading-edge semiconductors and the engineering and design services needed to make AI functional. These technologies, however, are also products and services with their own commercial value. The 2022 ban on exports to China of chips needed for AI, along with the services to design them and the machines to make them, was broadened in 2023 and reflects the difficult trade-offs and other choices U.S. policymakers face in safeguarding the United States’ technology resilience while supporting its commercial advance.⁸

As in the case of AI, Washington’s expanding definition of economic security is ensnaring a growing range of other technologies previously treated as commercial. New regulatory decisions about which technologies to impose controls on and at what levels hold immense implications for U.S. firms that expect to reap the commercial opportunities from new products and services (or to license or sell their innovations). These restrictions also have new ramifications for foreign firms and states. Foreign firms that are already licensed to import U.S.-controlled goods are subject to rules with penalties to prohibit re-exporting these goods and technologies to hostile states in their own products and services. Washington’s broader new limits on commercial goods and services add to a wider array of legal limits and are creating some new surprises for leading private firms.

⁷ “Treasury Issues Regulations to Implement Executive Order Addressing U.S. Investments in Certain National Security Technologies and Products in Countries of Concern,” U.S. Department of the Treasury, Press Release, October 28, 2024.

⁸ “Commerce Implements New Export Controls on Advanced Computing and Semiconductor Manufacturing Items to the People’s Republic of China (PRC),” U.S. Bureau of Industry and Security, Press Release, October 7, 2022; and “Commerce Strengthens Restrictions on Advanced Computing Semiconductors, Semiconductor Manufacturing Equipment, and Supercomputing Items to Countries of Concern,” U.S. Bureau of Industry and Security, Press Release, October 17, 2023.

Re-making Trade and Inventing New Industrial Policies for Economic Resilience

The semiconductor sector, as both a key target for resilience policies in the first dimension and the main vehicle to implement these policies for other technologies such as AI, reflects the United States' quest for economic resilience in the second dimension: the elevated priority placed on greater industrial self-reliance and reduced dependence on supply from abroad. To accomplish these goals, the United States now utilizes tariffs, subsidies, and other measures as incentives to spur production at home (reshoring/onshoring), along with other efforts to mitigate supply chain risks from abroad (diversification). U.S. efforts to promote industrial resilience represent a marked departure from past practice as the United States turns away from its traditional approach of openness to free trade toward a stronger emphasis on policies for direct reshoring. These trends will only accelerate as the second Trump administration begins to implement its own agenda and vision to achieve a similarly defined goal.

The Biden administration identified semiconductors early in its term among a short list of designated “critical and essential” goods for U.S. economic security, along with six key industrial sectors (defense, health and biological preparedness, information technology and communications, transportation, energy, and food), as priority areas for new reshoring and supply chain diversification initiatives.⁹ These issues are complex and unique in each area, necessitating extensive and multifaceted steps to achieve resilience. Nonetheless, some patterns in U.S. policy preferences have emerged. To highlight the intent, tools, and direction of the United States' new efforts to increase the country's industrial resilience, this subsection considers key measures taken in three of the designated products and sectors—semiconductors, electric vehicles (EVs), and solar products.

Semiconductors. For the semiconductor sector, the Biden administration, with significant bipartisan support, identified reshoring chip production to reduce supply dependence on China as a top priority for increasing U.S. industrial resilience. To accomplish this goal, the administration kept in place the Trump administration's 25% tariffs on chip imports from China and later doubled these tariffs in 2024 to 50%. With tariffs in place to insulate the U.S. market and local producers from imports from China, the administration worked to secure bipartisan congressional passage of the 2022 CHIPS and Science Act, which added \$30 billion in subsidies as incentives for private firms to construct plants that produce leading-edge chips in the United States, as well as related inputs and components deemed at risk of disruption. To qualify to receive subsidies under the CHIPS Act, private companies must agree to a long list of eligibility requirements, most notably limits on expansion of their chip business operations involving China—reflecting the deep concern that excessive exposure to China poses risks to U.S. resilience.

While the process of shifting semiconductor supply chains, particularly through the construction of new fabs, is inherently slow, these government-led efforts have taken additional time to get off the ground. Nonetheless, manufacturing incentives were allocated after two years, and construction is underway on several large new semiconductor plants in the United States. Once online, these factories will substantially increase U.S.-based production capacity, especially in high-end chips, which stood at only 12% of global output at the time the 2022 CHIPS Act was passed.¹⁰ Whether maintaining tariff walls or adding billions more in U.S. government subsidies

⁹ “Securing America's Critical Supply Chains,” White House, Fact Sheet, Press Release, February 24, 2021.

¹⁰ Semiconductor Industry Association, “2022 Factbook,” May 2022, i–ii, https://www.semiconductors.org/wp-content/uploads/2022/05/SIA-2022-Factbook_May-2022.pdf.

will be necessary to sustain this scale of new chip investments, jobs, and production in the United States into the next generation of chip production will emerge as a new test of Washington's long-term commitment to securing industrial resilience (via direct reshoring) in this sector.

The administration also engaged allies and other chipmaking nations through dialogues to strengthen resilience in the sector, beginning with securing stable supply chains for the inputs necessary for chip manufacturing. These dialogues initially focused on improving information sharing, with limited progress made toward more concrete outcomes. Ultimately, the signals these efforts send to adversarial countries like China could prove to be their most important function—blunting China's potential to leverage its exports to coerce nations dependent on them. This web of new chipmaking alliances forged by the United States has established principles of stable, predictable, and diversified supply chains as a basic starting point.

Electric vehicles. The Biden administration adopted similar approaches to promote U.S.-based production of EVs, along with efforts to diversify supply chains away from dependence on China for EV batteries. As with semiconductors, the Biden administration embraced the Trump administration's tariffs of 25% (raised from 2.5%) on imported automobiles from China. Then, in 2024 the Biden administration announced a further increase in tariffs on EVs from China up to 100%.

The administration also worked for passage in 2022 of the Inflation Reduction Act (IRA), which includes billions of dollars in government subsidies to encourage production of EVs and associated batteries in the United States. Compared with the CHIPS Act, which focused on subsidies for new manufacturing, the IRA's subsidies seek to increase demand for domestically produced EVs through generous tax credits to U.S. consumers and businesses for EV purchases. To support more EV production in the United States, the subsidies also set broad criteria to exclude most foreign-made goods from qualification. EVs must be produced in North America and EV batteries must be produced either in North America or in a limited number of allied or partner countries to be eligible.

Numerous U.S. trading partners, from allies and adversaries alike, sharply criticized Washington for overtly discriminatory criteria excluding most foreign goods, calling it a plain-letter violation of the United States' nondiscrimination commitments under international trade rules. Even as China continued to subsidize its own EV industry, it filed a complaint at the World Trade Organization over U.S. subsidies. Meanwhile, other countries with major EV manufacturers attempted to keep up by establishing their own subsidy programs, often with explicit domestic preferences.

This choice to prioritize domestic manufacturing through discriminatory subsidies, which is precisely the kind of race that the United States has traditionally aimed to avoid, reflects the preeminence the Biden administration gave to industrial reshoring over other objectives to increase resilience.¹¹ The Biden administration often defended these EV subsidies as an essential policy tool to meet U.S. climate obligations. Yet the decision to disqualify most imports from receiving the IRA subsidies might slow the rate of EV adoption and thus undercut U.S. efforts to mitigate climate change.

¹¹ As one indication of the new U.S. priorities, in 2009, to help the auto industry recover after the 2007–8 global financial crisis, Congress approved a tranche of consumer tax-break subsidies for purchases of vehicles that met higher environmental standards. Domestic preferences like those included in the 2022 IRA were considered but ultimately rejected in favor of nondiscrimination in treatment of U.S.- and foreign-made automobiles under the 2009 program.

Solar products. Policies to bring solar industry production back to the United States reflect a similar mix of choices to those made for EVs and semiconductors. These efforts have been routinely updated to stay apace of rapid changes in market conditions for this industry. Global production of solar products is highly concentrated in China and affected by its dominance and policies that include enormous state subsidies and allowance of deeply problematic labor practices.

Both the Trump and Biden administrations have relied on large tariff hikes on imports—increasing and decreasing these as industry dynamics have changed—to help revive and bolster the fragile U.S. solar industry. These restrictive measures have been accompanied by tax break subsidies under the IRA for residential and commercial solar panel installation, along with additional incentives for purchases of U.S.-made panels. The IRA also includes subsidies for companies that invest in new U.S. manufacturing capacity for solar and other clean energy-related products. The survival of U.S. producers facing significantly higher production costs than many international competitors might require long-term political support to sustain tariffs. When set against the economic and environmental costs of a slower and costlier rollout of solar products, these policy choices reflect the superseding priority the U.S. government is placing on promoting resilience in the form of domestic manufacturing and reshoring over other policy objectives.

The cases of semiconductors, EVs and EV batteries, and solar products epitomize the character of the United States' search for industrial resilience. As a slogan lent political relevance by the outsized electoral priority placed on support for manufacturing jobs, “resilience” has been used in a malleable way to encompass goals ranging from domestic production to supply chain security to climate change mitigation. Among them, reshoring efforts often have taken precedence. Tariff protection, generous subsidies, and other measures continue to redefine U.S. trade policy priorities and spur new U.S. industrial policies. These choices are unprecedented during the United States' postwar history—both for the sharpness in turn toward industrial planning, protection, and market intervention for commercial goods and for the turn away from support for open, nondiscriminatory global trade.

Supply chain diversification and security initiatives were the other key hallmarks of the Biden administration's approach to industrial resilience. These were manifested through domestic efforts, ranging from supply chain “mapping” to real-time information sharing and reporting on imports among U.S. ports. International efforts range widely and included bilateral and minilateral engagements to diversify supply chains and facilitate more informed coordination. Each was pursued with the stated goal of increasing the capacity of the United States, or of its allied members, to minimize future disruptions from pandemics, natural disasters, military conflicts, or other unanticipated global developments. The future of these various efforts under the second Trump administration is unclear.

A New Economic Resilience

The United States' new search for economic resilience has been motivated by a range of objectives, including environmental, political, economic, and security concerns. Many of these, particularly those connected to technological leadership, have been given increased impetus by the rise of China as an economic and strategic competitor. Others, however, are principally driven by deeper goals, such as greater industrial self-reliance.

The United States, due to its size, influence, and technological leadership, drove the global agenda in economic security for 75 years. For sensitive technologies, it developed a “high fence, small yard” approach to control its most important know-how and military hardware. Principally in response to China’s technological and military ascendancy, the United States has made this fence higher and this yard larger, seeking to bring along other countries in line with its controls. In nonsensitive areas, Washington had pursued a rules-based approach for nearly 75 years to foster greater trade interdependence, but it is now turning away from this approach to prioritize other goals. These new trade policy choices, which often aim to serve an agenda and priorities that are domestically driven, will only dramatically accelerate under the second Trump administration.

Due to the United States’ size and powerful position in both global technology and trade, these choices also will create uncertainty for the rest of the world and have an impact on U.S. foreign interests and relations. For the United States, closer cooperation and coordination with allies and other leading nations in advanced technology, such as Japan, whose approach to economic security and resilience is discussed in a separate essay in this report, is essential to meet the growing technological and economic security risks posed by China and others. Even as many of their core interests are often aligned, U.S. decisions on which additional dual-use technologies to limit and which ordinary commercial good imports to discourage from abroad will further test the United States’ ability to forge new and maintain existing commercial and other alliances with these nations. Where differences in threat perceptions or traditional commercial interests exist, U.S. allies increasingly are likely to find themselves, if not by choice then by unilateral action, expected to “pick a lane”—whether between the strategic and military interests of the United States and China or between acquiescence to Washington’s new trade barriers and insistence on adherence to the international trade rules and system.

The Biden administration attempted to seek acceptance by other nations of its “economic resilience” priorities and encouraged them to join the United States to pursue “similar approaches and build alignment and complementarity across our policies and our investments.”¹² The second Trump administration will likely pursue new technological and economic security priorities with greater unilateralism and assertiveness. Thus, as the United States redefines its national self-interest, even though specific tactics might change, the broad shift in U.S. economic strategy toward resilience is likely to persist.

¹² “Remarks by APNSA Jake Sullivan at the Brookings Institution,” White House, October 23, 2024.

The Strategic Role of Japan's Development Finance under the New Dimension of Digital Infrastructure

Hiroyuki Suzuki

HIROYUKI SUZUKI is Deputy Director General of the Corporate Planning Department and a Startup Investment Committee Member at the Japan Bank for International Cooperation (JBIC). He can be reached at <hiro-suzuki@jbic.go.jp>.

EXECUTIVE SUMMARY

This essay argues that the rapid expansion of the digital economy has made the development of reliable digital infrastructure in both developed and developing countries critical to ensuring digital resilience.

MAIN ARGUMENT

China is increasing its presence in global digitalization efforts through the Belt and Road Initiative, and in response the United States and like-minded partners in Europe and Asia are developing new digital infrastructure strategies as a countermeasure. Given the strength of Japanese industry in the digital domain, strengthening Japan's digital infrastructure efforts should be an important factor. In fact, the Japanese government is in the process of developing a new infrastructure strategy, and support for digital infrastructure and the digital transformation (DX) is expected to be one of the pillars. While the Japan Bank for International Cooperation, Japan's development finance institution, has been expanding its support for the efforts of Japanese companies in the digital area, such as subsea cables and data centers, through cooperation with the U.S., Australia, South Korea, and other like-minded countries, more work must be done to continuously and strategically enhance ongoing projects. In recent years, as the expansion of digital demand, including for artificial intelligence (AI), has caused power consumption to rapidly increase, the integration of DX and green transformation (GX) has been progressing, adding another critical set of policy considerations to digital infrastructure financing.

POLICY IMPLICATIONS

- Like-minded countries should utilize development finance institutions strategically to strengthen their support for the development of digital infrastructure, with cooperation between actors in the private and public sectors.
- Taking into account the huge increase of power demand stemming from the development of AI, support for digital infrastructure should be further developed by integrating DX and GX.
- Global standards for quality infrastructure should be updated promptly, especially considering the rapid expansion of generative AI.

With the increasing adoption of digital and telecommunications technologies around the world, the enormous demand for data is growing rapidly on a global scale. Digital transformation (DX) has become both the center of fierce competition among global companies and one of the major challenges in the economic development of the global South. In this regard, the digital sector has become a key pillar of economic growth in both developed and emerging economies.

In recent decades, the People's Republic of China (PRC) has been a leading player in digital infrastructure development in the global South, especially by providing financial and technical support through the Digital Silk Road Initiative as part of its broader Belt Road Initiative (BRI). These efforts, and the resulting digital foothold the PRC has gained in the digital ecosystems of developing markets, have spurred other major economic powers to increase their commitment to compete in this domain. The Partnership for Global Infrastructure and Investment (PGII), a U.S.-led G-7 infrastructure cooperation platform, and the European Union's Global Gateway have emerged as leading alternatives to China's infrastructure development programs. Japan has also been very active in digital areas. Recently, the synergies between the digital sector and conventional infrastructure projects have also become key in the economic corridors supported by PGII, such as the Lobito Corridor linking the Democratic Republic of the Congo, Angola, and Zambia to the Port of Lobito, the Luzon Economic Corridor in the Philippines, and others.¹ Beyond these government-level initiatives, U.S. and Japanese companies are significantly expanding collaboration in such vital areas as submarine cables, 5G, and Open RAN (Open Radio Access Network).

Because of the increased importance of the sector, ensuring that the underlying digital infrastructure is resilient has become a key policy objective for Japan, the United States, and others. This essay examines the Japanese government's policies toward digital infrastructure development and the strategic trends emerging in the digital sector as Japanese firms carry out projects with financial assistance from the Japan Bank for International Cooperation (JBIC). It concludes with a discussion of recent developments that are expected to further strengthen expansion and cooperation in this sector.

Japan's International Digital Development Strategy and the New Digital Infrastructure Initiative

In Japan's overarching vision of its place among the world's democratic nations, the country hopes to play a role in bridging the gap on economic and technology policy between the two poles of the EU and the United States. Recognizing the importance of data and the digital infrastructure across which it flows, former prime minister Shinzo Abe announced his vision of Data Free Flow with Trust to the world in 2019.² Since then, Japan's efforts have continued, though they remain a work in progress. While large, primarily U.S. private-sector companies are leading the way in the field of data on the internet, Japan is expected to have the potential to accelerate the utilization of real data, especially industrial data to stimulate innovation. The country's focus on digital

¹ "Partnership for Global Infrastructure and Investment Lobito Corridor: Supporting Transcontinental Connectivity," U.S. Department of State, September 24, 2024, <https://www.state.gov/partnership-for-global-infrastructure-and-investment-lobito-corridor-supporting-transcontinental-connectivity>.

² World Economic Forum, "Data Free Flow with Trust (DTFF): Paths Towards Free and Trusted Data Flows," White Paper, May 2020, https://www3.weforum.org/docs/WEF_Paths_Towards_Free_and_Trusted_Data%20_Flows_2020.pdf.

infrastructure construction reflects an effort to lean into these national advantages and carve out a role for Japan in the global digital ecosystem.

While private-sector cooperation is integral to fostering resilient infrastructure, in order to further strengthen these strategic Japanese and U.S. corporate partnerships, the role of development finance institutions (DFIs) such as JBIC and the U.S. Development Finance Corporation (DFC) is becoming more immediate and vital. Likewise, the United States and Japan continue to support aligned strategic-level policy dialogues in multilateral frameworks, such as the Competitiveness and Resilience (CoRe) Partnership and the Quad (with Australia and India).³ Meanwhile, on its own initiative and with the support of the Japanese government, JBIC is expected to be increasingly capable of helping implement relevant Japanese and U.S. private-sector projects in like-minded countries, leveraging public-private partnerships to increase resilience.⁴

As mentioned above, utilizing JBIC's financial support, Japanese companies are accelerating their global expansion in the digital sector. The government of Japan is also preparing a new strategy in response to these developments. In 2024, it developed a new infrastructure strategy for the year 2030, and during the National Council for Infrastructure Cooperation Strategy, held on June 5, 2024, three strategy pillars were articulated:⁵

- Enhancing Japan's "earning power" and international competitiveness, responding to the needs of partner countries, and creating projects together, including in new areas that go beyond the conventional infrastructure concept, opening up the world's economic prosperity.
- Securing supply chains, economic security, and national interests, including by closely cooperating with like-minded countries and the global South.
- Achieving sustainable growth for Japan and the world through agile responses to green, digital, and other social transformations that will become major growth markets and opportunities.

The following items are specifically stated for the digital sector, indicating that this sector is a key pillar of the plan:

- In order to secure the national interest, Japan will focus on developing critical infrastructure in the digital sector, including 5G/Open RAN, optical submarine cables, and data centers. In addition to strategically acquiring orders for peripheral infrastructure that supports this infrastructure through public and private financing, Japan will support the necessary human resource development. In doing so, care will be taken to ensure that there is no risk of illegal functions being embedded in infrastructure equipment or used as a means of sabotage.
- The G-7 countries will promote efforts to realize safe, secure, and reliable AI through the Hiroshima AI Process launched during Japan's G-7 presidency in 2023 and lead the development of sustainable digital infrastructure to support the explosive growth in demand for AI.
- In the area of critical infrastructure for economic security, Japan will further strengthen cooperation with like-minded countries through proactive risk-taking.
- To strengthen public finance as a complement to private finance, Japan will establish various mechanisms, such as blended finance, that appropriately combine public and private financing.

³ "U.S.-Japan Competitiveness and Resilience (CoRe) Partnership," White House, Fact Sheet, April 16, 2021, <https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/16/fact-sheet-u-s-japan-competitiveness-and-resilience-core-partnership>.

⁴ See the May 2021 issue of JBIC Today, available at https://www.jbic.go.jp/en/information/today/image/jtd_202105.pdf.

⁵ See *Keikyo infra senryaku kaigi* [Japan's National Council for Infrastructure Cooperation Strategy] (Tokyo, 2024).

The prioritization of resilience is immediately evident in the above points. Ensuring that critical infrastructure necessary to preserve economic security is resilient against risks of sabotage or other malicious use is a central part of efforts to minimize disruptions across these networks. Moreover, as AI-enabled applications increasingly leverage advanced digital infrastructure and the cross-border flow and storage of data, ensuring that these applications are safeguarded against misuse is also a key part of achieving broader resilience objectives. Finally, as shown in the above examples, public-private partnerships inherently result in more resilient, sustainable project concepts. With the above in mind, it will be important for both the public and private sectors to work together with the United States and other like-minded countries. Japan has already been making significant progress toward these goals through JBIC's efforts to support public-private cooperation across the global South. The following section highlights several examples of these efforts and the impact they are achieving.

Japan's Digital Infrastructure Development in Practice

As Japan's DFI, JBIC is the key actor in supporting the strategic global expansion of Japanese companies, in a manner linked to government-level initiatives. Recently, the number of projects that JBIC is supporting in the digital sector has expanded through increased cooperation with like-minded countries, including the United States. As the following examples show, the development of digital infrastructure has also become a core component of Japan's efforts to strengthen ties with the global South.

Japan-U.S.-Australia Collaboration: Submarine Cables in Palau

In January 2021, JBIC concluded a \$4 million buyer's credit loan agreement with the Belau State Submarine Cable Corporation.⁶ The loan was the first project under a November 2018 trilateral memorandum of understanding between the U.S., Japanese, and Australian DFIs and was issued to finance the purchase of submarine cable-related equipment from NEC. The trilateral partnership on infrastructure investment targeting the Indo-Pacific aims to realize individual projects in which Japanese, U.S., and Australian companies collaborate in the region. The three partners highlighted that the priority for these projects was to advance infrastructure development on terms that adhere to high global standards and are built to last while enhancing the resilience and self-sufficiency of host countries.⁷

By supporting a project such as this one, the three countries' DFIs provided a strong signal in support of resilient digital infrastructure. The fact that the project was announced by the foreign ministers of the three countries at the Indo-Pacific Business Forum reflects the importance of the project. The loan will strengthen the telecommunications infrastructure of Palau, a vital Indo-Pacific island nation, and will contribute both to expanding telecommunications capacity and to improving the overall stability of international telecommunications.

⁶ "Buyer's Credit for State-Owned Submarine Cable Corporation of Palau," JBIC, Press Release, January 14, 2021, <https://www.jbic.go.jp/en/information/press/press-2020/0114-014143.html>.

⁷ "JBIC Signs MOU with U.S. International Development Finance Corporation," JBIC, Press Release, April 12, 2024, https://www.jbic.go.jp/en/information/press/press-2024/press_00005.html.

Japan-U.S.-Australia Collaboration: South Pacific Telecommunications Operators

Building off the above success in trilateral efforts to support resilient digital infrastructure, both JBIC and the U.S. DFC in March 2023 concluded separate \$50 million agreements with Export Finance Australia, covering a portion of its loan to Telstra Group, a major telecommunications operator in Australia. The agreement between the two Australian institutions supported the funding of the acquisition of Digicel Pacific, a local mobile telecommunications operator in the South Pacific Islands region, by the Telstra Group.⁸

Digicel Pacific has a market share of over 60% in the Pacific Island countries, and therefore it plays a central role in the stability of the telecommunications sector in the region. In addition, Digicel Pacific has extensive telecommunications infrastructure in rural areas and is actively working to expand these networks. Absent these efforts, the reliability of rural networks and the connectivity they promote in these regions would be severely undermined. The importance of these secure and high-quality telecommunications networks was referenced in a joint press statement by the United States, Japan, and Australia on the sidelines of the G-20 in November 2022, which also recognized the importance of this financial assistance in realizing these policy objectives.⁹ The project's efforts to establish a reliable telecommunications network in the South Pacific region are part of a strategic initiative seeking to ensure the realization of a free and open Indo-Pacific region.

The South Pacific region has traditionally used inexpensive Chinese telecommunications equipment, which has raised concerns over the resilience of these networks in the face of potential risks. The Australian government intends to utilize the “trusted vendor” approach in the reconstruction of telecommunications networks to upgrade to 4G and 5G. This approach is based on the statement adopted at the Prague 5G Security Meeting held in May 2019, with participants from 32 countries, including Japan, the United States, and Australia. The statement highlighted as its first proposal that “communication networks and services should be designed with resilience and security in mind,” reflecting the importance of these objectives to a wide range of like-minded partners.¹⁰ The possibility of Japanese companies' participation is also expected to be enhanced, reflective of their long history of delivering resilient, secure infrastructure projects across the Indo-Pacific.

Japan-U.S.-ROK Cooperation: High-Level Meeting with the U.S. DFC and the Export-Import Bank of Korea for Cooperation in the Digital Sector

The partnerships among like-minded countries and their DFIs to boost private-sector cooperation in the digital infrastructure sector are also becoming more active as part of the commitment to trilateral cooperation between the United States, Japan, and the Republic of Korea (ROK) that emerged out of the Camp David Summit in April 2023. In March 2024, JBIC agreed with the U.S. DFC and the Export-Import Bank of Korea (KEXIM) to consider and deepen cooperation for the development of India's digital infrastructure in order to further strengthen the

⁸ “Joint Statement by Australia, Japan and the United States on Telecommunications Financing,” U.S. DFC, Press Release, May 19, 2023, <https://www.dfc.gov/media/press-releases/joint-statement-australia-japan-and-united-states-telecommunications-financing>.

⁹ “United States-Australia-Japan Joint Statement on Cooperation on Telecommunications Financing,” White House, November 15, 2022, <https://www.whitehouse.gov/briefing-room/statements-releases/2022/11/15/united-states-australia-japan-joint-statement-on-cooperation-on-telecommunications-financing>.

¹⁰ “Prague 5G Security Conference Announced Series of Recommendations: The Prague Proposals,” Government of the Czech Republic, May 3, 2019, <https://vlada.gov.cz/en/media-centrum/aktualne/prague-5g-security-conference-announced-series-of-recommendations-the-prague-propos.als-173422>.

trilateral partnership.¹¹ The three institutions signed a memorandum of understanding pledging to continue discussions to support the development of such digital infrastructure by making full use of the various financial tools of each institution.

Global internet traffic is expected to be 30 times as high in 2030 as in 2021, placing significant strain on the digital infrastructure that is an important driving force in economic development. The burden will be especially heavy in India, where the information and communications technology (ICT) sector accounts for more than 13% of GDP.¹² India also plans to develop its digital infrastructure at the national level and increase its ICT sector to a trillion-dollar scale by 2025.

In April 2024 the three institutions held discussions directly with India's Ministry of Electronics and Information Technology and confirmed that they would collaborate on measures to develop India's digital infrastructure. The three organizations introduced the ministry to Japanese, U.S., and South Korean technologies and initiatives related to digital infrastructure and discussed ways to promote future cooperation possibilities. The participants agreed to continue discussions to support the development of India's digital infrastructure, including 5G, Open RAN, data centers, and smart cities, by making full use of various financial tools.¹³

Japan-U.S.-ROK Cooperation: Loan for the Data Center Business of the NTT Group in India

This dialogue between Japan, the United States, and the ROK has led to actual project support with the Indian market in mind. In March 2024, JBIC concluded an agreement with NTT Global Data Centers and Cloud Infrastructure India, an Indian subsidiary of NTT, for a loan of 10.2 billion rupees to support data center construction and operation in Maharashtra.¹⁴

The Indian government for its part has set forth a plan to make India a hub for data centers in its Data Center Policy 2020. It also is promoting business through preferential measures and the establishment of special economic zones, in both financial and nonfinancial terms. These policies have facilitated India's rise as a regional data center hub—a trend that is expected to continue as the volume of data communication further increases with the expansion of generative AI, e-commerce, social media, and other uses.¹⁵

Export Credit Line for the Development Bank of Angola

In 2016, JBIC signed an agreement with Banco de Desenvolvimento de Angola, the national bank of the Republic of Angola, for a loan of approximately \$65.8 million to finance the purchase of a complete optical submarine cable system by a domestic telecommunications operator directly

¹¹ "DFC (U.S.), KEXIM (Korea), and JBIC (Japan) Seek to Strengthen Their Coordinated Approach to Digital Transition during their High-Level Trilateral Meeting in Tokyo," JBIC, Joint Statement, March 6, 2023, https://www.jbic.go.jp/ja/information/topics/topics-2023/image/20240306_the_Joint_Statement.pdf.

¹² "JBIC Signs Arrangement with U.S. International Development Finance Corporation and Export-Import Bank of Korea," JBIC, Press Release, October 28, 2024, https://www.jbic.go.jp/en/information/press/press-2024/press_00090.html.

¹³ "DFC, JBIC, and Korea Eximbank Expand Partnership with India through New Framework to Promote Digital Infrastructure Initiatives," U.S. DFC, Press Release, October 25, 2024, <https://www.dfc.gov/media/press-releases/dfc-jbic-and-korea-eximbank-expand-partnership-india-through-new-framework>.

¹⁴ "Loan for Data Center Business of NTT Group in India," JBIC, Press Release, April 19, 2024, https://www.jbic.go.jp/en/information/press/press-2024/press_00007.html.

¹⁵ "India to be a Cloud Computing and Data Centre Hub," Press Information Bureau (India), December 8, 2022, <https://static.pib.gov.in/WriteReadData-specificdocs-documents-2022-dec-doc2022128141601.pdf>.

connecting Angola and Brazil.¹⁶ This project is the world's first optical submarine cable to connect the African and South American continents across the southern Atlantic Ocean. It will also connect to a submarine cable leading from Brazil to the United States, thereby establishing a communications network from Angola to North America. The cable will use the world's most advanced technology in terms of transmission capacity, connectivity, and expandability, establishing a high-quality telecommunications infrastructure network from Africa to countries in South America and improving the resilience of Angola's and the region's access to telecommunications. Disruption to undersea cables off the coasts of West and South Africa earlier this year led to internet outages across the continent. By establishing more novel routings for connectivity, this project will mitigate the risk of future disruptions.

Future Challenges

While the emergence of Japan's new infrastructure strategy reflects the great opportunities the Japanese government perceives in supporting the rollout of resilient digital infrastructure, current projects are being influenced by geopolitical risks, the gap between public interest and the actions of major platform companies (e.g., Google, Apple, Meta, and Amazon), the development of generative AI, and synergies with decarbonization. This section discusses these challenges and their implications.

The Geopolitical Movements of Platforms for Submarine Cables

A key aspect of establishing a secure and resilient digital ecosystem in the Indo-Pacific is the expansion of undersea cable networks to connect data centers to consumption areas. Given that AI requires large amounts of power, data centers of the future are likely to be selected in regions with large and stable supplies of electricity, especially green power. This presents challenges for regions such as the Pacific Islands where data centers are not commercially viable. In these cases, undersea cables will play an increasingly important role and often will require public funds. U.S. and Japanese public-private partnerships are working to address this challenge.

While routes for laying submarine cables were previously decided among governments and operators, recently major platform companies have begun taking the lead in investing in new projects to meet the massive demand for data. In fact, several submarine cables connecting the United States to the Indo-Pacific, Latin America, and Europe are being planned and constructed, mainly through projects in which platform companies are investing. This includes multiple submarine cables in the Indo-Pacific to connect the United States with Southeast Asia in order to bypass chokepoints such as the South China Sea.¹⁷

In this context, Japan, Hong Kong, and Singapore have become intra-Asian hubs, and Australia and the ROK are emerging as hubs as well. In addition, due to hurdles resulting from the need to seek permission from China to lay cables in the South China Sea, as well as to technological advances in submarine cables, several submarine cables have been planned in recent years to connect the United States to Southeast Asia via Australia.

¹⁶ "Export Credit Line for Development Bank of Angola," JBIC, Press Release, March 31, 2016, <https://www.jbic.go.jp/en/information/press/press-2015/0331-47541.html>.

¹⁷ "Big Tech and Geopolitics are Shaping the Internet's Plumbing," *Economist*, December 20, 2023, <https://www.economist.com/business/2023/12/20/big-tech-and-geopolitics-are-reshaping-the-internets-plumbing>.

In addition, there are growing concerns about economic security risks associated with submarine cables, such as the risk of cable cuts and information leaks, and addressing these risks is also important. In response to this situation, the Japan-U.S.-Australia-India Partnership for Cable Connectivity and Resilience was announced in the joint statement from the Quad summit in May 2023. The partnership is expected to be linked to infrastructure support.¹⁸ Other major challenges include delays in landing country licensing and tight submarine cable repair and maintenance capacity. The latter, in particular, is a poorly profitable business, and therefore the availability of concessional financing will be an important aspect of future digital infrastructure development. The mobilization of private capital through blended finance is expected to play a critical role in addressing this challenge.

The Convergence of Digital Transformation and Green Transformation

Currently, leading U.S. tech and AI companies are investing in data centers in new markets. With the advent of the AI era, the data center market size is expected to reach \$440 billion in 2028 (a 40% increase over 2022), and demand for GPUs, the main type of semiconductor used in AI applications, is expected to reach 18 times the 2022 level in the next ten years.¹⁹ Over 90% of the market is currently dominated by AI chips packaged by Nvidia in the United States, SK Hynix in the ROK, and TSMC in Taiwan.

As mentioned above, low-cost clean power supplies are needed for data centers that consume enormous amounts of electricity. Specifically, electricity demand for data centers and other facilities will double between 2022 and 2026, according to the International Energy Agency, reaching a level comparable to Japan's current electricity demand.²⁰ On the other hand, U.S. tech companies, which dominate AI semiconductors, have set a goal of using renewable energy to cover the power consumed by their data centers, and the challenge will be how to secure stable, clean power at low cost. They are setting their sights on the Indo-Pacific region as a new market for AI development and investments in data centers.²¹ In terms of lowering the cost of power, India, Malaysia, and Australia are promising options. The United States is expected to strategically promote reduced reliance on China, using its own technology as leverage and continuing to restrict the flow of advanced technologies to China.

Trends around the decarbonization of power sources will continue to push industry toward the fusion of green transformation (GX) and DX. To this end, host countries could provide competitive subsidies for renewable energy to attract investment in data centers for the promotion of innovation in AI. In the global South, in particular, it is important to promote business opportunities for the energy transition by utilizing advanced technologies in the development of renewable energy sources and power grids. Given the vast amount of investment that will be required, DFIs like JBIC will need to play a leading role in supporting the rollout of these modern grids. It is important that policymakers remember that such grids are not just an energy or environmental question but also inextricably linked to digital infrastructure issues.

¹⁸ "The Wilmington Declaration Joint Statement from the Leaders of Australia, India, Japan, and the United States," White House, Press Release, September 21, 2024, <https://www.whitehouse.gov/briefing-room/statements-releases/2024/09/21/the-wilmington-declaration-joint-statement-from-the-leaders-of-australia-india-japan-and-the-united-states>.

¹⁹ "AI Power: Expanding Data Center Capacity to Meet Growing Demand," McKinsey, October 29, 2024, <https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/ai-power-expanding-data-center-capacity-to-meet-growing-demand>.

²⁰ International Energy Agency, "Electricity 2024: Analysis and Forecast to 2026," Report, January 2024, <https://www.iea.org/reports/electricity-2024>.

²¹ Author's conversations with a U.S. tech company.

The Development of Digital Governance and Infrastructure Standards

In December 2023 the “Hiroshima AI Process G-7 Digital and Technology Ministerial Statement” was adopted at the G-7 Digital and Technology Ministerial Meeting, building on the leader-level initiative outlined at the May 2023 summit in Hiroshima. The statement presents the first international guidelines for generative AI, as well as a work plan to promote the Hiroshima AI Process. It focuses on risks that have been a concern for generative AI, such as the proliferation of disinformation, and calls for improved literacy, cooperation in vulnerability detection, and information sharing to ensure that digital networks remain resilient in the AI era. The statement also establishes a work plan to achieve these goals, including outreach to countries that are not members of the G-7 and the introduction of monitoring tools for companies and others to patrol the guidelines, in addition to the formulation of international guidelines. Italy took over the promotion of the Hiroshima AI Process as the G-7 president in 2024, but it remains to be seen whether the process will be integrated with the governance of infrastructure support. Given the critical role of digital infrastructure in the adoption of AI at scale, coordination between these governance mechanisms is of utmost importance.

Regarding the governance of infrastructure support, Japan also participates in the Blue Dot Network framework, which was developed as a tool to operationalize high-level principles of resilience at the actual project level.²² The Blue Dot Network offers certification based on economic, social, governance, and environmental criteria intended to provide investors and stakeholders with credible indicators that a project is sustainable, resilient, open, transparent, and efficient. The ultimate goal is to ensure the high quality and resilience of infrastructure investments made by like-minded partners, which were agreed on at the G-20 summit hosted by Japan in 2019. Certification will make projects more appealing to investors and serve to facilitate fundraising. It is also expected to simplify environmental, social, and governance reporting; improve evaluation by stakeholders such as construction contractors and project developers; and secure advantages in bidding. In addition, for governments and local communities, certification will promote sustainable development and infrastructure investment.

The secretariat has been established, and the certification process has begun. The Blue Dot Network is also considering the establishment of a digital platform, further simplification of certification procedures for projects involving multilateral development banks and DFIs, and support for developing countries. Building off the framework provided by the Hiroshima AI Process to create global standards for the role of AI in digital infrastructure that can be put into practice through the network in the future will be another test of the viability of the public-private partnership approach exemplified by the Blue Dot Network.

Conclusion

While Japan is increasing its engagement in the digital sector and infrastructure development, it will be important for the country to develop a strategy that is linked to geopolitical realities as well as to broader industrial supply chains and access to the semiconductors and data centers needed

²² Blue Dot Network, “Blue Dot Network Certification Framework,” April 9, 2024, <https://static1.squarespace.com/static/65fd77fec4ad696366329acd/t/6639dfc746f3b664a741cc2e/1715068873022/Blue+Dot+Network+certification+framework.pdf>.

to fuel digital growth. Any new strategies should also include clean energy and decarbonization as key components.

It will also be important for the public and private sectors to work together to develop digital governance that takes into account the development of generative AI. Technology in the digital field is advancing at an extremely rapid pace. Effective public-private partnerships that accurately take this into account will be required. DFIs, including JBIC, will need to continue their efforts to enhance cooperation between the private and public sectors, collaborating with like-minded countries.

As digital infrastructure is entering a new dimension under DX and GX, both the public and private sectors should recognize that responding quickly to new developments will provide direct opportunities to enhance resilience and find solutions to geopolitical disruptions. The catalytic function of DFIs in bridging the public and private sectors, if used to move strategically, boldly, and quickly, will be critical for unlocking this potential.

THE NATIONAL BUREAU *of* ASIAN RESEARCH

NBR SPECIAL REPORT #116 | FEBRUARY 2025

Japan's Cybersecurity Resilience Efforts in Collaboration with the United States

Mihoko Matsubara

MIHOKO MATSUBARA is Chief Cybersecurity Strategist for the NTT Corporation in Tokyo, where she is responsible for cybersecurity thought leadership. She served at the Japanese Ministry of Defense before completing an MA at the Johns Hopkins School of Advanced International Studies on a Fulbright scholarship. Prior to joining NTT, she worked as vice president and public sector chief security officer for the Asia-Pacific at Palo Alto Networks. She is an awarded author of two books on cybersecurity and the war in Ukraine. She can be reached at <tga@nbr.org>.

EXECUTIVE SUMMARY

This essay examines Japan's efforts to bolster its cybersecurity and resilience, prompted by the outbreak of the war in Ukraine in February 2022, its growing concerns over a potential conflict in the Taiwan Strait, and the major ransomware attack on the Port of Nagoya in July 2023.

MAIN ARGUMENT

Japan is currently working to enhance its cybersecurity and resilience. Not only has it passed legislation on active cyberdefense to minimize the damage caused by substantive cyberattacks that can compromise national security, but it also has established new requirements for critical infrastructure companies to enhance their cybersecurity practices under the revised Economic Security Promotion Act. These and other efforts will require legal initiatives and domestic and international public-private partnerships through the legislation on active cyberdefense, the government sharing intelligence on cyber threats with industry, threat-hunting collaboration, and global law-enforcement cooperation to disrupt cyberattacks. While the defeat suffered by Prime Minister Shigeru Ishiba's ruling coalition in the October 2024 election could delay some legislative efforts, the country has been proactively contributing to global resilience through law-enforcement collaboration to disrupt ransomware criminal activities and its participation in an international annual cyber exercise with Australia, the United Kingdom, and the U.S. By bringing not only the Japan Self-Defense Forces and Ministry of Defense but also civilian agencies and critical infrastructure companies to the exercise, these initiatives enable Japan to serve as a regional hub for cybersecurity and resilience collaboration and better prepare for major disruptive cyberattacks on critical infrastructure services during a national security crisis.

POLICY IMPLICATIONS

- While Japan's legislation on active cyberdefense tends to attract attention to offensive capabilities, it is equally important for Japanese policymakers to increase the country's defensive capabilities through secure-by-design and secure-by-default strategies, as well as by providing support for under-resourced small and medium-sized businesses.
- The Japanese government should establish a procedure to declassify cyber threat intelligence to share with industry stakeholders, so that individuals without a security clearance can use the intelligence to better protect their assets and contribute to national security and resilience.
- The government needs to create a legal framework to issue a waiver from regulatory requirements for companies to accept its threat-hunting offer. Otherwise, companies that are concerned about potential legal risks if government threat hunters find a gap between their cybersecurity practices and regulatory requirements will decline to participate in government initiatives.

Cybersecurity is one of the major pillars in Japan's economic and national security. The country is increasingly aware of the need for cyber resilience to prepare for the potential of disruptive or destructive cyberattacks after three wakeup calls: the Russian invasion of Ukraine in February 2022, which included cyber elements; the ransomware attack on the Port of Nagoya in July 2023, which paralyzed cargo shipping operations for two days; and potential cyber disruptions to critical infrastructure if conflict were to occur in the Taiwan Strait.

The ongoing war in Ukraine has reminded Japan that cyberattacks are an integral part of modern war and that long-term cyber resilience efforts—through international public-private partnerships—can drastically strengthen national cyberdefense capabilities even against formidable adversaries.¹ The cyberattack on the Port of Nagoya also prompted Japan to take measures to enhance the cybersecurity resilience of critical infrastructure services to help achieve broader economic security goals.

This essay analyzes the current cyber threat landscape and Japan's efforts to strengthen its cybersecurity capabilities and resilience. Under the 2022 National Security Strategy, the Japanese government is developing new legislation on active cyberdefense to minimize the damage to the country's national security that would be caused by a substantive cyberattack, or even to neutralize a cyberattack before it is launched. The essay explores ongoing Japan-U.S. collaboration in the field and considers next steps the allies could take.

The Current Cyber Threat Landscape Facing Japan and the United States

Japan's 2022 National Security Strategy states that the primary cybersecurity threats consist of disruptive or destructive cyberattacks on critical infrastructure services and nonkinetic operations precursive to armed attacks as part of hybrid warfare.² Such nonkinetic operations include both cyberattacks and information operations. For example, Russia reportedly embedded wiper malware in the network of Ukrainian Railways prior to its invasion in February 2022. A cybersecurity team from the U.S. Army's Cyber Command, defense contractors, and private cybersecurity firms, however, were able to discover and delete the malware when they visited the country in late 2021. This threat-hunting effort prevented devastating damage to Ukraine's capabilities to conduct civilian evacuations, provide humanitarian aid, and organize military logistics in wartime.³

Since the outbreak of the war in Ukraine, Japan has become increasingly worried about potential conflict in the Taiwan Strait. Upon the release of the 2022 National Security Strategy, Prime Minister Fumio Kishida revealed at a press conference that the government had conducted realistic simulations to test Japan's current defense capabilities and stated that the results indicated the country's capabilities were insufficient for deterrence or defense. He called for Japan to

¹ Yuster Yu and Mihoko Matsubara, "Taiwan and Japan Must Learn from Russian Cyberwarfare," *Nikkei Asia*, January 25, 2024, <https://asia.nikkei.com/Opinion/Taiwan-and-Japan-must-learn-from-Russian-cyberwarfare>.

² Government of Japan, *National Security Strategy of Japan* (Tokyo, December 2022), 6, <https://www.cas.go.jp/jp/siryoku/221216anzenhoshou/nss-e.pdf>.

³ Mehul Srivastava, Madhumita Murgia, and Hannah Murphy, "The Secret U.S. Mission to Bolster Ukraine's Cyber Defences Ahead of Russia's Invasion," *Financial Times*, March 9, 2022, <https://www.ft.com/content/1fb2f592-4806-42fd-a6d5-735578651471>. Wiper malware deletes data and files in the infected systems and prohibits the victim from accessing the data and files, which can not only paralyze the business operations of the victim organization but also create cascading effects for other companies through supply chains.

strengthen its cyber, space, and electromagnetic capabilities as the line between peacetime and wartime is becoming increasingly blurry due to growing use of hybrid warfare. With both the prime minister and the National Security Strategy emphasizing the Japan Self-Defense Forces (JSDF) defense posture in the Ryukyu Islands, it was clear that a potential Taiwan crisis was the motivating concern.⁴

If China invades Taiwan, the operation is expected to include a large number of cyberattacks. U.S. FBI director Christopher Wray pointed out that China has been studying lessons from the war in Ukraine—including those relating to cyberwarfare—to prepare for a Taiwan contingency.⁵ The U.S. Office of the Director of National Intelligence predicted in its 2023 threat assessment that China “almost certainly would consider undertaking aggressive cyber operations against U.S. homeland critical infrastructure and military assets worldwide” to distract U.S. decision-making, create chaos, and prevent the deployment of the U.S. military if a major conflict with the United States were imminent.⁶

Such preparation seems to be underway in the cyber domain. In fact, the U.S. government announced in January 2024 that a Chinese state-sponsored group of actors called Volt Typhoon had targeted the U.S. “communications, energy, transportation, and water sectors” and that U.S. law enforcement disrupted the Chinese botnet.⁷ Unfortunately, the Volt Typhoon operations are ongoing. Lumen Technologies, a U.S. telecommunications firm, revealed in August 2024 that it had detected a series of cyberattacks against four U.S. companies and one Indian company in the information technology (IT) sector, which it attributed with moderate confidence to Volt Typhoon.⁸ Furthermore, Volt Typhoon breached Singapore Telecommunications in June 2024, and this hack seems to have been intended to test its capabilities to prepare for future cyberattacks against U.S. telecommunication companies and other foreign critical infrastructure companies.⁹

A major challenge with Volt Typhoon stems from difficulties in detecting its cyberattacks due to the use of stealthy “living-off-the-land” tactics. In a living-off-the-land attack, the adversary uses legitimate administration tools to evade detection but is still able to steal information and escalate privileges to access more sensitive data.¹⁰ For example, the U.S. government admitted that Volt Typhoon hackers maintained their malicious access to victims for at least five years in some cases.¹¹ This is a very long time for an attacker to remain undetected, allowing it to collect a large amount of information for future cyber operations.

⁴ “Kishida Naikaku Sori Daijin Kisha Kaiken” [Press Conference by Prime Minister Kishida], Prime Minister’s Office of Japan, December 16, 2022, https://www.kantei.go.jp/jp/101_kishida/statement/2022/1216kaiken.html.

⁵ “FBI: Iran Govt Hackers Targeted U.S. Children’s Hospital,” Agence France-Presse, June 1, 2022, <https://www.france24.com/en/live-news/20220601-fbi-iran-govt-hackers-targeted-us-children-s-hospital>.

⁶ Office of the Director of National Intelligence, “Annual Threat Assessment of the U.S. Intelligence Community,” February 6, 2023, 10.

⁷ “U.S. Government Disrupts Botnet People’s Republic of China Used to Conceal Hacking of Critical Infrastructure,” Office of Public Affairs, U.S. Department of Justice, Press Release, January 31, 2024, <https://www.justice.gov/opa/pr/us-government-disrupts-botnet-peoples-republic-china-used-conceal-hacking-critical>.

⁸ “Taking the Crossroads: The Versa Director Zero-Day Exploitation,” Black Lotus Labs, Lumen Technologies, August 27, 2024, <https://blog.lumen.com/taking-the-crossroads-the-versa-director-zero-day-exploitation>; and Lawrence Abrams, “Chinese Volt Typhoon Hackers Exploited Versa Zero-Day to Breach ISPs, MSPs,” Bleeping Computer, August 27, 2024, <https://www.bleepingcomputer.com/news/security/chinese-volt-typhoon-hackers-exploited-versa-zero-day-to-breach-isps-mmps>.

⁹ Jordan Robertson and Katrina Manson, “Chinese Group Accused of Hacking Singtel in Telecom Attacks,” Bloomberg, November 5, 2024, <https://www.bloomberg.com/news/articles/2024-11-05/chinese-group-accused-of-hacking-singtel-in-telecom-attacks>.

¹⁰ “Cybersecurity Advisory: People’s Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection,” U.S. Cybersecurity and Infrastructure Security Agency, May 24, 2023, <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a>.

¹¹ “Cybersecurity Advisory: PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure,” U.S. Cybersecurity and Infrastructure Security Agency, February 7, 2024, <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a>.

In addition, U.S. law enforcement conducted its second disruption of the Chinese hacking efforts in September 2024. In this instance, another group of Chinese state-sponsored hackers, Flax Typhoon, had infected more than 200,000 consumer devices, such as routers and surveillance cameras, to steal sensitive information and position themselves for future disruptive cyber operations. Approximately half of the infections were in the United States, but the affected devices were spread around the world, including in Vietnam, Germany, and India.¹²

The U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency deployed its threat-hunting team to "water, power, energy, and transportation" companies 97 times in fiscal year 2023 alone to "find and eradicate" Chinese cyber operations, while also publishing more than 1,100 cybersecurity advisories.¹³ Although it remains unknown whether those threat-hunting operations found any indications that Chinese hackers had compromised critical infrastructure, a public-private partnership would allow the U.S. government and industry to clarify the needs of critical infrastructure companies to strengthen their cyberdefenses and foster mutual trust for closer cooperation.

Furthermore, ransomware attacks have posed serious threats to economic and national security for both the United States and Japan, as well as more broadly around the globe. A cybersecurity company based in the United Kingdom, Sophos, conducted a survey across fourteen countries in 2024 and found that 59% of respondents experienced ransomware attacks over the previous year.¹⁴

Even when a financially motivated criminal group targets a single company, that cyberattack can create cascading impacts on multiple industrial sectors through supply chain disruptions. For example, the 2023 ransomware attack on the Port of Nagoya caused the port—the largest commercial port in Japan—to suspend its cargo shipping operations for two days.¹⁵ As critical infrastructure becomes increasingly digitized, the risks of cyberattacks having disproportionate impacts on societal resilience rise, while the distinction between financially motivated and state-sponsored disruptive attacks diminishes. Given the importance of privately owned critical transportation infrastructure such as ports, railways, and airports for military deployment during a crisis, it is unsurprising that these companies remain priority targets—whether in Ukraine or the Indo-Pacific. That is why it is imperative for those firms and the government to collaborate to increase their cyberdefenses and resilience so that victims can resume their business operations quickly.

Japan's Efforts to Promote Cybersecurity and Resilience

Japan has taken steps to strengthen its cybersecurity and resilience by passing the Economic Security Promotion Act (ESPA) and by shifting toward an active cyberdefense policy under the 2022 National Security Strategy. Given that cyberattacks are borderless and damages can spread

¹² "Court-Authorized Operation Disrupts Worldwide Botnet Used by People's Republic of China State-Sponsored Hackers," U.S. Department of Justice, Press Release, September 18, 2024, <https://www.justice.gov/opa/pr/court-authorized-operation-disrupts-worldwide-botnet-used-peoples-republic-china-state>; and "Joint Cybersecurity Advisory: People's Republic of China-Linked Actors Compromise Routers and IoT Devices for Botnet Operations," U.S. Internet Crime Complaint Center, September 18, 2024, 4.

¹³ "Opening Statement by CISA Director Jen Easterly," Cybersecurity and Infrastructure Security Agency, April 30, 2024, <https://www.cisa.gov/news-events/news/opening-statement-cisa-director-jen-easterly-0>.

¹⁴ Sophos, "The State of Ransomware 2024," April 2024, 3.

¹⁵ Sean Lyngaas, "Japan's Largest Port Hit with Ransomware Attack," CNN, July 6, 2023, <https://edition.cnn.com/2023/07/06/tech/japan-port-ransomware-attack/index.html>.

beyond national borders, Japan is also expanding international collaboration on cybersecurity, as will be discussed in detail in the next section.

First, the Port of Nagoya incident reminded Japan of the importance of securing essential services, which include critical infrastructure, from disruptive cyberattacks to protect supply chains. Although the port was not designated as essential infrastructure at the time of the attack, Economic Security Minister Sanae Takaichi suggested this change immediately after the incident,¹⁶ and the Japanese government later designated ports and associated logistics infrastructure as essential infrastructure as part of revisions to the ESPA in May 2024.¹⁷

Furthermore, the ESPA designates that 210 companies across fifteen sectors of essential infrastructure services, such as electric power and finance, are required to submit relevant information to the government. This includes the name of companies that manufactured their key systems and the location, board members, and major shareholders of those manufacturers. Companies must also describe the measures they are taking—including cybersecurity—to manage potential risks of disruption to their essential services before the designated service providers deploy key systems in their facilities or contract maintenance work for those systems. If the government identifies any major risks that are not addressed in the provided information, the ESPA permits it to require that essential infrastructure service providers modify their approach or stop deploying the systems. This kind of government audit of critical infrastructure aims to ensure continued stable operation of essential infrastructure services.¹⁸

Second, under the 2022 National Security Strategy, Japan is establishing a new mandate for active cyberdefense to promote cyber resilience against attacks that pose a serious threat to national security. The government will seek to disable such cyberattacks even if they do not constitute an armed attack, aiming to minimize the damage they can cause to Japan or its critical infrastructure. While the Japanese government has yet to define the scope of active cyberdefense or specific cases in which its use would be triggered, the mention of the term in the strategy implies the necessity of some offensive capabilities to neutralize potential cyberattacks against Japan. The National Security Strategy suggests that the government should help critical infrastructure service providers with gathering intelligence and responding to incidents, as well as collaborate with telecommunication service providers and use their data to detect compromised servers utilized by adversaries.¹⁹

In June 2024 the Japanese government established a panel of experts to discuss what other legislation is needed to materialize active cyberdefense.²⁰ According to an interim report in August 2024, the panel members suggested that active cyberdefense entails a whole-of-society resilience approach by supporting small and medium-sized businesses for better cybersecurity

¹⁶ “Kikan infura jizen shinsa, kowan tsuka wo kento Takaichi Keizai Anpo-sho” [Economic Security Minister Takaichi Suggested to Consider Adding Port to a Subject of Mandated Previews for Critical Infrastructure], *Nikkei*, July 14, 2023, <https://www.nikkei.com/article/DGXZQOUA149P90U3A710C2000000>.

¹⁷ “Takaichi Naikakufu Tokumei Tanto Daijin kisha kaiken yoshi Reiwa 6 nen 5gatsu 17 nichi” [Press Conference by Minister Takaichi on May 17, 2024], Cabinet Office, May 17, 2024, https://www.cao.go.jp/minister/2309_s_takaichi/kaiken/20240517kaiken.html.

¹⁸ “Kikan infura no shinsa kaishi = saiba kogeki boshi—Seifu” [The Government Started Preliminary Review of Designated Essential Infrastructure Service Providers to Prevent Cyberattack Damages], *Jiji Press*, May 17, 2024; and Cabinet Office, “Outline of the Essential Infrastructure System and Required Information: Operation of the System Commences on May 17, 2024,” July 2024, https://www.cao.go.jp/keizai_anzen_hosho/suishinhou/infra/doc/pamphlet_itaku_eng.pdf.

¹⁹ Government of Japan, *National Security Strategy of Japan*, 23–24.

²⁰ “Expert Panel toward Improving Response Capabilities in the Field of Cybersecurity,” Prime Minister’s Office of Japan, June 7, 2024, https://japan.kantei.go.jp/101_kishida/actions/202406/07cyber.html.

and increasing adoption of secure-by-design and secure-by-default practices.²¹ While active cyberdefense often attracts attention to the offensive elements of the approach, defensive elements are equally important. The government cannot respond to every single cyberattack with active cyberdefense, since some attacks will not meet the threshold to justify a government response. Thus, incorporating security from the beginning through secure-by-design and secure-by-default practices is a constructive way to enhance resilience. Furthermore, the government needs to help under-resourced small and medium-sized businesses, given their important role to play in supply chains.

While the panel noted the need to analyze telecommunications data to understand the scope of cyberattacks, it also asked for legislation to balance public welfare, the constitutional requirement to protect the secrecy of communications, and human rights. Public welfare includes national security needs, but the panel discussions did not clarify how to draw a line between national defense and privacy concerns. The panel also recommended the establishment of an independent organization to audit data collection and usage.²²

Prime Minister Shigeru Ishiba had stated that his administration would accelerate its efforts to submit legislation on active cyberdefense as soon as possible, based on the discussions by an expert panel during a Upper House plenary session on October 8, 2024.²³ The cabinet approved the proposed legislation on active cyberdefense, and it was sent to the Diet on February 7, 2025. The Japanese government is keen to pass the bills during the regular session of the Diet and implement them.²⁴ Yet Prime Minister Ishiba's coalition of the Liberal Democratic Party and Komeito lost the snap election held in late October 2024, with no party winning a majority of seats in the Diet. Thus, the defeat could prevent the Diet from smoothly passing the bills.

International Public-Private Collaboration

To deal with cyberattacks that can easily transit international borders and that utilize and target private-sector devices and technology, international public-private partnerships are indispensable. Sharing cyber threat intelligence and best practices to minimize damages is crucial, as is conducting joint exercises to test communication channels and incident response capabilities in real-world scenarios.

Japan became a member of the NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) in November 2022,²⁵ and even prior to membership, it had begun working with the center through its annual cyber exercises, Locked Shields, to practice responses to large-scale disruptive cyberattacks on critical infrastructure services. In April 2021 the Japanese team competed in the cyber exercise for the first time. The delegation included the Ministry of Defense, the JSDF,

²¹ "Saiba anzen hoshō bunya deno taio noryoku no kōjo nimuketa yushikisha kaigi koremade no giron no seiri" [Interim Summary of the Discussions by the Panel of Experts on National Cybersecurity], Cabinet Secretariat, August 7, 2024, 3–5, https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo/giron_seiri/giron_seiri.pdf.

²² Ibid., 7–10.

²³ "Ishiba shusho, nodoteki saiba bogyo hoseibi wo kasoku Yato ha kiseiho saikaisei yokyuu Sanin daihyo shitsumon" [Prime Minister Ishiba Said His Administration Would Accelerate Its Efforts for Active Cyber Defense, but the Opposition Party Demands to Re-revise the Political Money Control Act during an Upper House Plenary Session], *Sankei Shimbun*, October 8, 2024, <https://www.sankei.com/article/20241008-CWZK43FGSZOOV14TTD5LK2EGV4>.

²⁴ "Japan Govt. Approves Draft Legislation to Forestall Cyberattacks," NHK World, February 7, 2025, https://www3.nhk.or.jp/nhkworld/en/news/20250207_16.

²⁵ "NATO saiba boei kyoryoku senta no katsudo heno seishiki sankā nitsuite" [Officially Joined NATO CCD COE Activities], Ministry of Defense (Japan), November 4, 2022, <https://www.mod.go.jp/j/press/news/2022/11/04b.html>.

the Ministry of Internal Affairs and Communications, the Information Technology Promotion Agency, the Japan Computer Emergency Response Team Coordination Center, and private-sector critical infrastructure companies.²⁶ Japan's team partnered with the U.S. Indo-Pacific Command, highlighting the robust alliance between the two countries. The partnership allowed them to assess their capabilities to jointly deal with disruptive cyberattacks on the financial sector, mobile information and communications technology services, and water supplies and to practice coordinating their responses between military and civilian agencies and multiple private critical infrastructure companies.²⁷

Given that a potential Taiwan contingency might begin with cyberattacks to disrupt critical infrastructure services and consequently military assets and deployment in the region, it is indispensable for Japan and the United States to build up their resilience and cyberdefenses together and with other like-minded countries. Since the 2021 exercise, Japan also worked with the UK Ministry of Defence in Locked Shields 2022 and 2024 and with Defence Australia in Locked Shields 2023.²⁸ These experiences have bolstered cyberdefense coordination between like-minded U.S. allies, with Japan serving as a hub for regional and global collaboration.

Besides international military cooperation in the context of joint exercises, Japan has also been contributing to global law-enforcement efforts to address ransomware threats. In October 2021, following the fallout from the Colonial Pipeline attack, the White House launched the Counter Ransomware Initiative. Approximately 30 allies and partners collaborated to disrupt the ransomware crime ecosystem through law-enforcement investigations and anti-money laundering measures.²⁹ As an inaugural member, Japan has taken an active role in supporting international investigations. For example, the Japanese National Police Agency aided international investigations into ransomware attacks on U.S. law-enforcement agencies and other organizations around the world, which led to the indictment of a Russian national in May 2023.³⁰ It also provided a decryption tool to help law enforcement from ten countries disrupt the malicious operations of the prolific LockBit ransomware group by closing its accounts, arresting its members, and shutting down its IT infrastructure.³¹ These experiences in working with other law-enforcement agencies will enable Japan not only to continue to support international efforts to combat ransomware threats but also to learn from other countries to more effectively target the malicious IT infrastructure and malign financial practices of cybercriminals.

²⁶ "NATO saiba boei kyoryoku senta niyoru saiba boei enshu 'Locked Shields 2021' heno sanko nitsuite" [Participating in NATO CCD COE's Cyber Exercise, "Locked Shields 2021"], Ministry of Defense (Japan), April 13, 2021, 1, <https://www.mod.go.jp/j/press/news/2021/04/13b.pdf>.

²⁷ Shannon Vavra, "NATO Tests Its Hand Defending Against Blended Cyber-Disinformation Attacks," CyberScoop, 2012, <https://www.cyberscoop.com/nato-blended-cyber-disinformation-defense-locked-shields-article-v>.

²⁸ "NATO saiba boei kyoryoku senta niyoru saiba boei enshu 'Locked Shields 2022' heno sanko nitsuite" [Participating in NATO CCD COE's Cyber Exercise, "Locked Shields 2022"], Ministry of Defense (Japan), April 19, 2022, <https://www.mod.go.jp/j/press/news/2022/04/19e.html>; "NATO saiba boei kyoryoku senta niyoru saiba boei enshu 'Locked Shields 2023' heno sanko nitsuite" [Participating in NATO CCD COE's Cyber Exercise, "Locked Shields 2023"], Ministry of Defense (Japan), April 18, 2023, <https://www.mod.go.jp/j/press/news/2023/04/18d.html>; and "NATO saiba boei kyoryoku senta niyoru saiba boei enshu 'Locked Shields 2024' heno sanko nitsuite" [Participating in NATO CCD COE's Cyber Exercise, "Locked Shields 2024"], Ministry of Defense (Japan), April 23, 2024, <https://www.mod.go.jp/j/press/news/2024/04/23c.html>.

²⁹ "Joint Statement of the Ministers and Representatives from the Counter Ransomware Initiative Meeting October 2021," White House, October 14, 2021, <https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/14/joint-statement-of-the-ministers-and-representatives-from-the-counter-ransomware-initiative-meeting-october-2021>.

³⁰ "Russian National Charged with Ransomware Attacks against Critical Infrastructure," U.S. Department of Justice, Press Release, May 16, 2023, <https://www.justice.gov/opa/pr/russian-national-charged-ransomware-attacks-against-critical-infrastructure>.

³¹ "Law Enforcement Disrupt World's Biggest Ransomware Operation," Europol, February 20, 2024, <https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation>.

Next Steps to Take

As Japan faces an elevated cyber threat environment with growing ransomware attacks and geopolitical tensions, it has undeniably taken significant steps to build up its cybersecurity capabilities and expand international collaboration. The government is adopting legislation on active cyberdefense so that it is better equipped to deal with cyber disruptions that can threaten national security. Furthermore, Japanese law enforcement's contribution to tackle ransomware attacks has been internationally recognized by the U.S. government and Europol. The Ministry of Defense and JSDF have been collaborating with critical infrastructure companies through their participation in international cyber exercises, in contrast with their counterparts in Australia, the UK, and the United States that have not brought in industry partners.

Moving forward, Japan should work to improve its threat-hunting capabilities and increase the government's ability to share intelligence on cyber threats with companies. So far, there has been no public report of the Japanese government conducting any threat-hunting engagements. Since the Ministry of Defense and JSDF acknowledged the importance of threat hunting in the Defense Buildup Program for risk management and plan to provide cybersecurity assistance for other entities,³² new legislation on active cyberdefense could allow the JSDF to more readily provide threat-hunting engagements to protect national security against cyber disruptions targeted at critical industries.

However, if the government wishes to provide this kind of threat hunting for private companies, measures will need to be taken to address industry concerns over potential liabilities. For instance, government threat hunters often identify gaps between current cybersecurity procedures and regulatory requirements for a company's networks. While companies may initially agree to accept threat hunting, if the industry becomes more worried about potential legal trouble following the government's involvement, companies will reject such offers from the government. Therefore, a framework for issuing waivers needs to be developed and agreed on with critical infrastructure companies before the government officially launches threat-hunting initiatives.

The expansion of security clearance to private-sector cybersecurity practitioners contributing to economic or national security objectives would make it easier for the Japanese government to share classified information on cyberattacks with industry partners. It is also crucial for the government to establish a procedure to desensitize and declassify cybersecurity information in a timely manner in crisis situations so that employees of critical infrastructure companies who do not hold a security clearance can take advantage of government intelligence to better defend their networks. Given the fast pace of potential crises, these policies must be in place upfront to have any effect.

Still, threat-hunting assistance does not need to always come from the government. Public-private partnerships often face delays due to legal and bureaucratic challenges. An increasing number of organizations across various sectors, however, are exploring direct information-sharing agreements. These agreements provide a framework for companies to collaborate proactively on cybersecurity issues while safeguarding their most critical assets.³³ Organizations can leverage these agreements to share information, tactics, and approaches in real time,

³² "Defense Buildup Program," Ministry of Defense (Japan), December 16, 2022, 11, 51, https://www.mod.go.jp/j/policy/agenda/guideline/plan/pdf/program_en.pdf.

³³ Author's email interview with David Beabout, September 30, 2024.

significantly enhancing their effectiveness. Even if not utilized regularly, these agreements ensure that organizations are prepared to respond far more swiftly in emergencies than government coordination typically allows.³⁴

The aforementioned initiatives would empower Japan to enhance its cybersecurity resilience. They would also contribute to the cybersecurity and resilience of the Japan-U.S. alliance as the world continues to be more connected and adversaries typically attack the weakest link. Increased resilience and collaboration are also essential to achieve broader regional and global cybersecurity objectives and minimize growing concerns over the Taiwan Strait.

³⁴ Author's email interview with David Beabout.

THE NATIONAL BUREAU *of* ASIAN RESEARCH

NBR SPECIAL REPORT #116 | FEBRUARY 2025

Countering Economic Coercion

Mariko Togashi

MARIKO TOGASHI is a Visiting Research Fellow at the Institute of Geoeconomics. Prior to her current position, she was a Research Fellow for Japanese Security and Defence Policy and a Matsumoto-Samata Fellow at the International Institute for Strategic Studies in London, focusing on Japan's economic security policy. She also worked at the Edwin O. Reischauer Center for East Asian Studies, focusing on the economic security of the United States, Japan, and China. She can be reached at <mariko.togashi@ihj.global>.

EXECUTIVE SUMMARY

This essay analyzes countermeasures to economic coercion both theoretically and practically and draws implications for Japanese strategy and U.S.-Japan cooperation.

MAIN ARGUMENT

The theoretical and technical challenges in assessing the effectiveness of countermeasures to economic coercion should not diminish the importance of such analysis. The freedom of countries to choose their own course of action without fear of being punished is the fundamental basis of the liberal international order. There are two main approaches to counter economic coercion: deterrence by denial and deterrence by punishment. While the latter is likely to be deployed more quickly and can be politically popular, the former offers a long-term solution and carries less risk of escalation. Japan has experienced two major cases of economic coercion since 2010 and countered them by diversifying either demand or supply. Both countermeasures have been generally effective. Japan has continued to develop preemptive and reactive measures, including passing the Economic Security Promotion Act in 2022 and leading international cooperation, especially with the U.S. Strengthening supply chains and creating collective mechanisms for managing times of disruption provide a long-term solution that has less negative impact than short-term retaliatory measures. Moreover, this approach advances Japan's broader foreign policy goal of protecting a free and open Indo-Pacific.

POLICY IMPLICATIONS

To maintain the momentum of their efforts to counter economic coercion collectively, the U.S. and Japan will need to address three potential challenges for policy coordination:

- The two countries' views on free trade have diverged in the past few years. While Japan still prioritizes the principles of free trade, the U.S. seems to have shifted away from traditional free-trade approaches.
- Whereas Japan focuses on denial strategies, U.S. policies traditionally rely on punitive measures.
- Japan and the U.S. could disagree on the meaning of strengthening supply chains or the definition of national security, driven by different degrees of protectionism in their economic and industrial policies.

Over the past decade, the use of economic coercion has increased significantly, resulting primarily from the People’s Republic of China (PRC) increasingly employing coercive measures as a tool to achieve its broader foreign policy objectives. Research shows that China has used economic coercion as many as 123 times from 2010 to 2022.¹ Examples include restrictions on salmon imports from Norway after the Nobel Committee selected Liu Xiaobo, who was convicted of inciting subversion of state power in China, as the recipient of the Nobel Peace Prize in 2010; limits on banana imports from the Philippines amid tensions in the South China Sea in 2012; and the closure of China-based stores belonging to Lotte, a major Korean retail chain, when South Korea decided to allow the United States to deploy the Terminal High Altitude Area Defense (THAAD) system in 2017.

Countering economic coercion has thus become a policy priority for many countries, including Japan and the United States. Japan gained first-hand experience with PRC economic coercion in 2010 when Beijing halted the export of certain rare earths to Japan following the detainment of a Chinese national whose fishing vessel collided with two Japanese coast guard ships in disputed waters. The experience led the country to become an early adopter of measures to mitigate risks and respond to coercion. Beyond the direct impact, economic coercion fundamentally challenges the rules-based international economic order, the defense of which is a top strategic priority for Japan. The United States, meanwhile, has vital interests in shaping and constraining the PRC’s behavior and ultimately emerging victorious in bilateral strategic competition.

Given their shared fundamental values, the size of their economies, and their historically strong ties, Japan and the United States have led the international effort to counter economic coercion. Although the overall macroeconomic impact of PRC economic coercion is often limited both qualitatively and quantitatively,² there would be detrimental consequences on multiple levels if the coercive actions were left unaddressed. On the business level, the economic costs could be significant, damaging the targeted industry. On the state level, even if the macroeconomic impact might be limited, the freedom to make decisions, especially for smaller economies, will be constrained (the so-called chilling effect of economic coercion). Finally, on the international level, the liberal economic order backed by the rule of law—the foundation of the “free and open Indo-Pacific” concept developed by Japan and supported by the United States—will be damaged.

This essay will deepen understanding of economic coercion and analyze countermeasures, focusing on Japanese strategy. Following this introduction, the first section provides an overview of economic coercion, including its theoretical underpinnings and the characteristics of modern economic coercion, and explores its effectiveness. The second section briefly examines deterrence theory to inform the effective development of countermeasures. The next section then analyzes countermeasures in practice, considering Japan’s two previous cases of being a target of economic coercion and its broader strategy to prevent the recurrence of this experience, including through increased international cooperation. Finally, the concluding section analyzes the benefits of the current path taken to counter economic coercion collectively and assesses potential challenges for U.S.-Japan leadership in the coming years.

¹ Aya Adachi, Alexander Brown, and Max J. Zenglein, “Fasten Your Seatbelts: How to Manage China’s Economic Coercion,” *Merics China Monitor*, August 25, 2022, https://merics.org/sites/default/files/2023-02/Merics_ChinaMonitor_EconomicCoercion_EN-4.pdf.

² Matthew Reynolds and Matthew P. Goodman, “Deny, Deflect, Deter: Countering China’s Economic Coercion,” Center for Strategic and International Studies, March 2023, https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-03/230321_Goodman_CounteringChina%27s_EconomicCoercion.pdf.

Understanding Economic Coercion

Definition of Economic Coercion

Although countries increasingly use and discuss the term “economic coercion,” there is no global consensus on its definition. The G-7 defines economic coercion as incidents that “seek to exploit economic vulnerabilities and dependencies and undermine the foreign and domestic policies and positions of member countries as well as partners around the world.”³ The European Union adopts a somewhat narrower definition of economic coercion as “a situation where a third country attempts to pressure the EU or a member state into making a particular choice by applying or threatening to apply, measures affecting trade or investment against the EU or a member state.”⁴

Theoretically, economic coercion is best understood as a specific form of economic statecraft,⁵ which David Baldwin defines as “governmental influence attempts relying primarily on resources that have a reasonable semblance of a market price in terms of money.”⁶ Daniel Drezner defines it as “the threat or act by a sender government or governments to disrupt economic exchange with the target state, unless the target acquiesces to an articulated demand.”⁷ Based on these theoretical underpinnings and the practical definitions used by organizations that have attempted to define economic coercion in the context of responding to it, this essay defines economic coercion as a tool of economic statecraft that exploits economic dependencies to influence behavior by imposing or threatening to impose economic costs.

The use of economic tools for foreign policy goals is by no means new, but there are a few characteristics that distinguish modern economic coercion from previous instances. First, the measures used in today’s economic coercion vary. China’s coercive approaches have been categorized into six types: popular boycotts, administrative discrimination, empty threats, legal defensive trade measures, trade restrictions, and tourism restrictions.⁸ Second, economic coercion today is often deployed through informal means, especially in the case of Chinese economic coercion. This is connected to the third feature, which is the vagueness of policy objectives. In many cases, China denies the causal relationship between the diplomatic, territorial, or strategic issues and the economic measures taken, rendering the policy objectives unclear. The fourth characteristic of modern economic coercion is that it leverages asymmetric economic dependencies in the globalized world. Today’s economic coercion is often referred to as a weaponization of economic interdependencies for this reason, making it harder to grasp the total effect of coercive measures.

Effectiveness of Economic Coercion

Measuring the effectiveness of economic coercion is a challenging empirical problem. Due to the vagueness of the policy objectives of Chinese economic coercion, it is not even easy to define—let alone measure—the success of a campaign. For instance, if China’s goal was to reverse

³ “G-7 Leaders’ Statement on Economic Resilience and Economic Security,” White House, Press Release, May 20, 2023, <https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/20/g7-leaders-statement-on-economic-resilience-and-economic-security>.

⁴ “Trade: Council Adopts a Regulation to Protect the EU from Third-Country Economic Coercion,” European Council, Press Release, October 23, 2023, <https://www.consilium.europa.eu/en/press/press-releases/2023/10/23/trade-council-adopts-a-regulation-to-protect-the-eu-from-third-country-economic-coercion>.

⁵ Reynolds and Goodman, “Deny, Deflect, Deter: Countering China’s Economic Coercion.”

⁶ David A. Baldwin, *Economic Statecraft* (Princeton: Princeton University Press, 1985).

⁷ Daniel W. Drezner, “The Hidden Hand of Economic Coercion,” *International Organization* 57, no. 3 (2003): 643–59.

⁸ Adachi et al., “Fasten Your Seatbelts.”

countries' targeted behavior, past instances show that most cases were not successful. However, if the goal was to impose costs on certain sectors or companies, alter the cost calculation, or intimidate nontargeted, smaller economies so that they will not act against Chinese interests, China might have been successful in many cases. In most of the cases, the targeted countries made some concessions but did not shift the course of their behavior completely. In 2010, for instance, Tokyo released the Chinese captain but did not apologize to Beijing as demanded. This case will be discussed in more detail later.

Even if the meaning of successful Chinese economic coercion could be defined, there are no set ways to measure the effectiveness of economic coercion, as is the case with economic sanctions. Sanctions are most likely to be successful (meaning the implementing country achieves its policy objectives) when the costs of defiance borne by the target are greater than its perceived costs of compliance. While this formula is simple, it is extremely difficult to measure these costs and the target's perception accurately.⁹ One analysis of 170 cases of economic sanctions since World War I argues that even if the sender's relative size and leverage are greater than those of the target, which is often the case in Chinese economic coercion, a campaign is only likely to be successful if the relative intensity of interest is higher for the sender than the target.¹⁰ In other words, as long as the target country is more determined to protect its interests than China is to target the country, the act of economic coercion is unlikely to be successful. Regarding other factors determining the effectiveness of economic coercion, a more recent study articulates several characteristics that make Chinese economic coercion less effective: the unilateral deployment, the relatively low cost imposed on the target country, the economic and political strength of the target, the targeting of adversaries, poor signaling, and lack of adequate inducements.¹¹

Among numerous variables that determine the costs of defiance (the willingness of the target country to bear the costs and not alter its course to align with Chinese interests), economic costs are one important element. While the economic costs imposed by Chinese coercion on specific sectors or companies can be significant, the macroeconomic costs tend to be limited. One study shows that the effect of a decrease in exports to China on the countries that received the Dalai Lama for an official visit at the highest level disappeared in the second year after the meeting.¹² That being said, given the complexity of today's economic interdependencies, measuring the ripple effect stemming from the disruptions of supply chains is arduous. For instance, during the pandemic, we saw how disruptions in the semiconductor supply chains could stop or delay the production of a variety of goods, such as automobiles, industrial machineries, smartphones, and computers. Therefore, when measuring economic costs to assess the effectiveness of Chinese economic coercion, indirect costs should be considered as well, which can potentially extend beyond the target economy.

Measuring the effectiveness of economic coercion is even more complicated when the impact of the so-called chilling effect on countries' decision-making is considered. Countries that are reliant on China economically or militarily might choose a course of action that is in line with its interests, sacrificing other national interests out of fear of potential coercion. The relative difficulty in measuring costs beyond simple macroeconomic indicators should not diminish their

⁹ Gary C. Hufbauer, Jeffrey Schott, and Kimberly Ann Elliott, *Economic Sanctions Reconsidered*, 2nd ed. (Washington, D.C.: Peterson Institute for International Economics, 2007), chap. 2.

¹⁰ Ibid.

¹¹ Reynolds and Goodman, "Deny, Deflect, Deter: Countering China's Economic Coercion."

¹² Andrea Fuchs and Nils-Hendrik Klann, "Paying a Visit: The Dalai Lama Effect on International Trade," *Journal of International Economics* 91, no. 3 (2013): 164–77.

importance when attempting to understand the effectiveness of economic coercion or develop countermeasures. The freedom of countries to choose their own course of action without fear of being punished is the fundamental basis of the liberal international order.

Countermeasures in Theory

From a theoretical perspective, countries can choose to pursue two approaches to counter economic coercion, as with any other coercive action: deterrence by denial and deterrence by punishment. Both approaches attempt to change the adversary's calculation, but the specific target in the adversary's decision-making process differs.

Deterrence by denial aims to dissuade an action by making it unlikely to succeed, thereby reducing the adversary's confidence that taking the coercive action will achieve its desired objectives. In short, deterrence-by-denial strategies seek to leverage the adversary's fear of failure to decrease the perceived benefit of its actions.¹³ Deterrence-by-denial strategies in the context of economic coercion include measures such as strengthening supply chains and establishing mechanisms to absorb the impact of economic coercion, such as by mitigating costs for affected businesses or by helping them find alternative markets. In pursuing such strategies in the context of economic coercion, countermeasures can be categorized into two types that are mutually reinforcing: preemptive and reactive measures.¹⁴ Preemptive measures seek to build economic resilience within the country and with partners, decreasing the asymmetric vulnerabilities that could be exploited as opportunities for economic coercion. Reactive measures are intended to mitigate the impact of economic coercion after the adversary's action.

On the other hand, deterrence-by-punishment strategies seek to prevent an action out of fear of retaliation by threatening consequences, raising the perceived cost of the action to the adversary.¹⁵ Examples of deterrence by punishment in the context of economic security include retaliation through sanctions, tariffs, and other restrictions. Since deterrence by punishment inherently develops countermeasures preemptively, credibility of threats is necessary for this approach to work. Comparing the two strategies, while the deterrence-by-punishment approach is likely to be deployed more quickly and can be politically popular as an active measure that imposes costs on an adversary, the deterrence-by-denial strategy offers a long-term solution and carries less risk of escalation.

Countermeasures in Practice: Japan's Denial Strategy

Japan's Experience and Reaction to Chinese Economic Coercion

In 2010 a Chinese fishing vessel collided with Japanese coast guard ships near the contested Senkaku Islands (known as the Diaoyu Islands in China). In response to the detention of the Chinese captain, China effectively halted rare earth exports to Japan.¹⁶ Despite clear evidence that

¹³ Reynolds and Goodman, "Deny, Deflect, Deter: Countering China's Economic Coercion."

¹⁴ Ibid.

¹⁵ Michael J. Mazarr, "Understanding Deterrence," RAND Corporation, Perspective, 2018, https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE295/RAND_PE295.pdf.

¹⁶ Oki Nagai, "No Compromise: How a Decade-Old Clash Points to China Today," *Nikkei Asia*, September 5, 2020, <https://asia.nikkei.com/Politics/International-relations/No-compromise-How-a-decade-old-clash-points-to-China-today>.

the captain's actions violated Japanese law, Japan released him to preserve the bilateral relationship and prevent escalation of the economic coercion. Given the reliance of Japan's tech-centric economy on rare earth minerals, the incident was a wake-up call for Japan regarding its high dependency on China to acquire certain strategic goods.

A month after Beijing effectively banned rare earth exports to Japan, Tokyo announced a comprehensive policy package to support the development and diversification of rare earth supplies, for which 100 billion yen (approximately \$1 billion at the time) was appropriated in the supplemental budget. The policy package added "advancement of the rare earth utilization industry" as a pillar alongside the four pillars already addressed in the Japanese government's supply strategy: (1) securing overseas resources, (2) promoting recycling, (3) developing substitution materials, and (4) building up stockpiles.¹⁷

Within a decade, Chinese rare earth minerals fell from around 90% of all Japanese rare earth imports to 60%.¹⁸ These efforts to reduce Japan's rare earth dependency on China are ongoing. In 2022 the Japanese Diet approved 6 billion yen for a project to extract resources for electric and hybrid vehicles in Minamitorishima, a coral atoll located approximately 1,900 kilometers southeast of Tokyo.¹⁹ Furthermore, in 2023 Japan acquired its first financial interest in mining heavy rare earth elements in Australia as part of this effort to reduce dependency on China. Sojitz, a Japanese trading firm, and the Japan Organization for Metals and Energy Security (JOGMEC) invested approximately A\$200 million in Australia's Lynas Rare Earths, which is the biggest non-Chinese rare earth mining company.²⁰

Despite the effective policy response and mitigation of risks in the rare earths sector, Japan once again became a target of Chinese economic coercion. In August 2023, shortly after Japan released treated water from the Fukushima Daiichi Nuclear Power Plant, China banned all imports of Japanese seafood. In 2022, it was the top destination for Japanese seafood, accounting for more than 20% of Japan's total seafood exports.²¹ A month after the ban, the market price of cold shellfish in Tokyo had decreased by 20%–30%, suggesting that even if coercion is assumed to have a limited macro-level impact, the effect on businesses can still be significant.²²

After the Chinese ban on Japanese seafood imports, several domestic and foreign government, scientific, and private-sector statements were made affirming the safety of Japanese seafood, and Japan took measures to increase domestic demand and diversify export destinations. The Ministry of Agriculture, Forestry and Fisheries, for example, announced a slogan for people to "eat five scallops per person."²³ Some sushi restaurant chains and Japanese websites for hometown tax—a tax system that encourages taxpayers in urban areas to pay their income taxes and residential taxes

¹⁷ Oshima Takeshi, "Reamataru shigen kakuho no genjo to kadai" [The Current Situation and Challenges in Securing Rare Metal Resources], Rippo to Chosa, December 2010, https://www.sangiin.go.jp/japanese/annai/chousa/rippou_chousa/backnumber/2010pdf/20101201043.pdf.

¹⁸ "Reaasu Nihon Taichu izondo nao rokuwari" [Japan's Rare Earth Dependency on China Still Around 60%], *Nikkei*, February 15, 2020, <https://www.nikkei.com/article/DGKKZO55674300U0A210C2EA2000>.

¹⁹ "Minamitorishimaoki de reaasu saikutsu e gijutsukaihatsu, nijuyonen nimo saikutsu kaishi" [Rare Earth Mining Technology to Be Developed Offshore of Minamitori-shima, Exploratory Mining to Begin in 2012], *Nikkei*, December 18, 2022, <https://www.nikkei.com/article/DGXZQOUA094KI0Z01C22A1000000>.

²⁰ Mamoru Tsuge and Shoya Okinaga, "Japan Takes First Stake in Heavy Rare Earths to Reduce China Reliance," *Nikkei Asia*, March 9, 2023, <https://asia.nikkei.com/Spotlight/Supply-Chain/Japan-takes-first-stake-in-heavy-rare-earths-to-reduce-China-reliance>.

²¹ "China's Ban on Japanese Seafood is Absurd," *Nikkei Asia*, August 30, 2023, <https://asia.nikkei.com/Opinion/The-Nikkei-View/China-s-ban-on-japanese-seafood-is-absurd>.

²² "Hotate souba V-ji kaifuku, Chugoku kinyu ichinen, hanro hirogari futatabi shinausu" [Scallop Market V-shaped Recovery One Year after the Chinese Embargo, Sales Channels Expanded, and Scallops Are Once Again in Short Supply], *Nikkei*, August 20, 2024, <https://www.nikkei.com/article/DGXZQOUB1469X0U4A810C2000000>.

²³ *Ibid.*

to rural municipalities instead of where they reside and to receive gifts in return—also launched campaigns to increase domestic demand. After these campaigns, household spending on scallops across Japan increased 1.5 times in the fourth quarter of 2023 compared with the same time period in 2022, according to a survey by the Ministry of Internal Affairs and Communications.²⁴ On top of domestic efforts to increase demand, Japan diversified its seafood exports. Year-on-year scallop exports to the United States increased by 64%, exports to Canada by 7.2 times, exports to Thailand by 3.5 times, and exports to Vietnam by 7.9 times.²⁵

Considering both examples, Japan's countermeasures to respond to Chinese economic coercion appear to have been generally effective. In the 2010 case, Japan limited the demand for the PRC's rare earths by developing domestic production and diversifying external supply channels. In the 2023 case, within a year the price of the banned scallops had returned to the same level as before the Chinese ban on Japanese seafood imports. These cases empirically show that for Japan the damage of economic coercion can be mitigated and overcome after a period of time, depending on the difficulty of replacing either the demand or the supply. Japan's experience, however, underscores the importance of having both the ability to deploy significant resources—which is more difficult for small or developing economies—and the policy resolve to do so.

Japan's Denial Strategy and International Cooperation

Building on its effective responses to these first-hand experiences as a target of economic coercion, Japan has continued to develop preemptive and reactive measures in recent years. In May 2022, it passed the Economic Security Promotion Act. One of the act's four pillars specifically focuses on building resilient supply chains. Various forms of financial subsidies are provided to approved companies with supply chain restructuring plans to help strengthen supply chain resilience, which in turn preemptively mitigates or deflects the impact of disruptions, including coercive ones.

Japan's concrete reactive measures are laid out in the Action Plan for Strengthening Industrial and Technological Foundation to Enhance Economic Security, which was announced in October 2023 and revised in May 2024 by the Ministry of Economy, Trade and Industry. Japan's approach in reactive measures is to utilize international frameworks and take actions based on international rules while supporting the private sector.²⁶ In supporting the private sector, Tokyo seeks to help companies develop and promote alternative overseas sales channels, provide technical assistance from experts through the Japan External Trade Organization, and cover the risks associated with the development of sales channels and losses for exchange rate fluctuations, controls on imports, and economic sanctions through Nippon Export and Investment Insurance.

In terms of international cooperation to counter economic coercion, the U.S.-Japan bilateral relationship has played a leading role. The two countries discussed ways to counter economic coercion at the first Japan-U.S. Economic Policy Consultative Committee Meeting (the Economic "2+2") in July 2022, including the need to act in coordination with other partners.²⁷ Since then,

²⁴ "Hotate souba V-ji kaifuku, Chugoku kinyu ichinen, hanro hirogari futatabi shinausu."

²⁵ Ibid.

²⁶ "Keizai anzenhoshou ni kansuru sangyou gijutsukiban kyooka akushon puran kaiteiban" [Revised Action Plan for Strengthening Industrial and Technological Infrastructure for Economic Security], Ministry of Economy, Trade and Industry, May, 2024, https://www.meti.go.jp/policy/economy/economic_security/240515actionplan.pdf.

²⁷ "Japan-U.S. Economic Policy Consultative Committee Meeting (the Economic '2+2')," Ministry of Foreign Affairs (Japan), Press Release, July 29, 2022, https://www.mofa.go.jp/na/na2/us/page6e_000296.html.

the United States and Japan have formed and developed multiple platforms to collectively counter economic coercion.

Reflecting the leadership of Japan in this area, one of the most significant developments took place during its G-7 host year, when participating leaders launched the Coordination Platform on Economic Coercion at the Hiroshima Summit in May 2023. The platform seeks to increase “collective assessment, preparedness, deterrence and response to economic coercion,” as well as “further promote cooperation with partners beyond the G-7.”²⁸ Concretely, within the coordination platform, the G-7 countries seek to “use early warning and rapid information sharing, regularly consult each other, collaboratively assess situations, explore coordinated responses, deter and, where appropriate, counter economic coercion, in accordance with our respective legal systems.” The importance of the coordination platform was reiterated during the following G-7 summit in Apulia, Italy, in June 2024.²⁹ The platform is a key tool for member states to counter economic coercion collectively, given their global political capital, technological advantage, and economic weight. Institutionalizing the platform is important so that these efforts can continue regardless of leadership changes.

Another major development in countering economic coercion collectively was agreed on among the United States, Japan, and South Korea at the Camp David Summit in August 2023. The three countries agreed to cooperate toward the launch of an early-warning system for information sharing and policy coordination to counter economic coercion.³⁰ The development under the trilateral platform is also significant, given the importance of the three economies for China, especially in terms of access to critical and emerging technology. Moreover, the fact that Japan and South Korea can work together as partners on this issue is likely to raise the cost of imposing economic coercion strategically within the region.

More broadly, other major groupings moving toward building resilient supply chains in the region include the Indo-Pacific Economic Framework for Prosperity (IPEF) and the Quad (Japan, Australia, India, and the United States). The U.S.-led IPEF Supply Chain Agreement, which went into effect in February 2024, was the first multilateral agreement on this issue. The agreement instructs member states to create action plans for critical supplies and allows them to use the crisis response network when facing a disruption.³¹ The Quad also has stood up working groups focused on supply chains in specific sectors, including clean energy and critical and emerging technology.³² These and other multilayered mechanisms to counter economic coercion are laying the foundation for major economies that have deep economic relations with China to act collectively in the event of economic coercion.

²⁸ “G7 Leaders’ Statement on Economic Resilience and Economic Security,” Ministry of Foreign Affairs (Japan), Press Release, May 20, 2023, <https://www.mofa.go.jp/files/100506815.pdf>.

²⁹ “Apulia G7 Leaders’ Communiqué,” G-7 Italy, June 14, 2024, <https://www.g7italy.it/wp-content/uploads/Apulia-G7-Leaders-Communique.pdf>.

³⁰ “The Spirit of Camp David: Joint Statement of Japan, the Republic of Korea, and the United States,” White House, Press Release, August 18, 2023, <https://www.whitehouse.gov/briefing-room/statements-releases/2023/08/18/the-spirit-of-camp-david-joint-statement-of-japan-the-republic-of-korea-and-the-united-states>.

³¹ “U.S. Department of Commerce Announces Upcoming Entry into Force of the IPEF Supply Chain Agreement,” U.S. Department of Commerce, Press Release, January 31, 2024, <https://www.commerce.gov/news/press-releases/2024/01/us-department-commerce-announces-upcoming-entry-force-ipef-supply-chain>.

³² “Quad Leaders’ Track Working Groups,” Department of the Prime Minister and Cabinet (Australia), 2023, <https://www.pmc.gov.au/resources/quad-leaders-summit-2023/quad-leaders-track-working-groups>.

Looking Ahead: U.S.-Japan Leadership in Collectively Countering Economic Coercion

Japan and the United States have made significant progress in building and developing multilateral platforms to counter economic coercion collectively in recent years. The initiatives the two countries have led to strengthen supply chains and create mechanisms for managing times of disruption are becoming more effective in mitigating and deflecting the impact of economic coercion arising from asymmetric economic dependencies. This simply means that Japan and like-minded countries now have fewer vulnerabilities that adversaries could exploit economically. As a result, such adversaries will be less likely to deploy economic coercion in the first place, which achieves the policy goal of preventing economic coercion without suffering the costs of either coercion itself or reactive responses to incidents. This approach provides a long-term solution, with less negative impact than short-term retaliatory measures that heighten economic disruption.

Moreover, strengthening supply chains and creating mechanisms that can be used in times of disruption advance Japan's broader foreign policy goal of protecting a free and open Indo-Pacific. Strengthening supply chains allows countries to counter economic coercion by appealing to the rule of law, which is the basis of the international liberal trade order, rather than deploying targeted retaliatory measures that can be criticized as discriminatory. This not only will prove more diplomatically or politically attractive to Japan's partners but also is more economically beneficial because it creates a predictable trade and business environment and contributes to greater overall economic security. In today's highly globalized economy, the ripple effect of unpredictable economic restrictions, such as export controls and investment restrictions, can hurt not only the economy of the country being targeted but also all that country's trading partners. Therefore, countering economic coercion in a way that does not hurt business relations is critical to achieving both economic security and economic growth. In this respect, building resilient supply chains and creating a system for collectively responding to disruptions provide a solution that achieves two potentially competing policy goals.

Although efforts by the United States and Japan have helped establish a foundation and facilitated international cooperation to counter economic coercion, it is now essential to maintain this momentum and institutionalize these measures both domestically and internationally. The biggest variable is leadership changes around the world, but especially in the United States. It is critical for like-minded countries to act collectively to counter economic coercion effectively, and therefore it will be essential that these bilateral and plurilateral efforts persist even as new leaders take office in participating countries. Unpredictable policy shifts in the United States have created uncertainty over its commitment to the IPEF as well as over U.S.-led efforts to work with partners and allies in the region to strengthen collective anti-coercion measures.

Institutionalizing international counter-coercion efforts both domestically and internationally will require looking beyond initial commitments and implementing more concrete domestic policies and regularized frameworks for international engagement. In this process, there are three potential challenges for U.S.- and Japanese-led initiatives to counter economic coercion collectively. First, there is a difference between the two countries' views on free trade. While admitting the need to adjust the existing system to better address new risks such as economic coercion, Japan continues to uphold the principles of free trade. On the other hand, the United States has implemented policies that demonstrate a shift away from traditional free-trade approaches, such as its withdrawal from what became the Comprehensive and Progressive

Agreement for Trans-Pacific Partnership, the launch of the IPEF as a keystone regional framework that lacked any form of binding trade liberalization, and the increased use of industrial policy. Several high-level officials during the Biden administration acknowledged this shift. U.S. Trade Representative Katherine Tai, for example, stated that “aggressive liberalization and tariff elimination” made the United States and other countries too dependent on China for critical materials and that “we are writing a new story on trade.”³³ In the same month, National Security Advisor Jake Sullivan called for measures to rebuild industrial capacity within the United States, shifting away from neoliberal assumptions and emphasizing the disadvantages of liberalization.³⁴

Second, Japan seems to put more weight on denial rather than punishment strategies than the United States does. The Japanese action plan on economic security clearly states the country’s focus on denial, while policy discourse in the United States—including the proposed Countering Economic Coercion Act, which includes punitive measures—suggests a high level of openness to the traditional U.S. reliance on punitive measures, such as tariffs and sanctions, as tools of economic statecraft.

Third, Japan and the United States could disagree on the meaning of strengthening supply chains or the scope of national security, driven by different degrees of protectionism in their economic and industrial policies. Although the two countries have managed their differences so far, such as through the clarification of the scope of the Inflation Reduction Act, the risk of divergence remains if the gap continues to widen.

Despite these differences, Japan and the United States both have strategic interests in countering economic coercion together and leading the international efforts. Regardless of the leadership, the cost of facing economic coercion without effective countermeasures is much higher than the cost of overcoming the differences between the two countries.

³³ David Lawder, “U.S. Trade Chief Tai Defends Pursuit of Non-traditional Trade Deals,” Reuters, April 5, 2023, <https://www.reuters.com/world/us/us-trade-chief-tai-defend-pursuit-non-traditional-trade-deals-2023-04-05>.

³⁴ “Remarks by National Security Advisor Jake Sullivan on Renewing American Economic Leadership at the Brookings Institution,” White House, Press Release, April 27, 2023, <https://www.whitehouse.gov/briefing-room/speeches-remarks/2023/04/27/remarks-by-national-security-advisor-jake-sullivan-on-renewing-american-economic-leadership-at-the-brookings-institution>.



Seattle and Washington, D.C.

600 UNIVERSITY STREET, SUITE 1012
SEATTLE, WASHINGTON 98101 USA
PHONE 206-632-7370, FAX 206-632-7487

1819 L ST NW, NINTH FLOOR
WASHINGTON, D.C. 20036 USA
PHONE 202-347-9767, FAX 202-347-9766

NBR@NBR.ORG, WWW.NBR.ORG