



Atlantic Council

SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

Toward resilience: An action plan for Taiwan in the face of PRC aggression

**Franklin D. Kramer, Philip Yu, Joseph Webster,
and Elizabeth Sizeland**





Atlantic Council

**SCOWCROFT CENTER
FOR STRATEGY AND SECURITY**

The **Scowcroft Center for Strategy and Security** works to develop sustainable, nonpartisan strategies to address the most important security challenges facing the United States and the world. The Center honors General Brent Scowcroft's legacy of service and embodies his ethos of nonpartisan commitment to the cause of security, support for US leadership in cooperation with allies and partners, and dedication to the mentorship of the next generation of leaders.



Atlantic Council

SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

Toward resilience: An action plan for Taiwan in the face of PRC aggression

**Franklin D. Kramer, Philip Yu, Joseph Webster,
and Elizabeth Sizeland**

Cover: Taiwan's landmark building Taipei 101 (center). REUTERS/Ann Wang

ISBN: 978-1-61977-342-4

This report is written and published in accordance with the Atlantic Council Policy on Intellectual Independence. The author is solely responsible for its analysis and recommendations. The Atlantic Council and its donors do not determine, nor do they necessarily endorse or advocate for, any of this report's conclusions.

July 2024

Table of Contents

Introduction	1
Establish a Comprehensive Security Strategy	2
Cybersecurity and critical infrastructure resilience	5
Energy	10
Enhancing defense resilience	16
Conclusion	20
About the authors	21
Acknowledgements	22

Introduction

This report recommends actions for the new leadership of Taiwan to take to enhance its societal resilience against Chinese aggression in the context of both “gray zone” conflict and wartime attacks. The brief focuses on establishing a comprehensive security strategy and analyzes three key areas particularly important for effective resilience: enhancing cybersecurity for critical infrastructures; improving energy security; and accelerating defense transformation.

The new administration of Lai Ching-te faces both existing resilience challenges and the potential for significantly greater problems if the People’s Republic of China (PRC) pursues expanded gray zone activities or if actual conflict occurs.¹ The ongoing challenges include substantial disinformation campaigns, cyberattacks, military incursions, and periodic economic coercion. Potential future challenges could involve expansion of one or more of these ongoing Chinese activities. In the context of a more contested environment such as a quarantine,² blockade, or a kinetic conflict, Chinese actions could seek to cause leadership failures and loss of social cohesion; undertake cyberattacks to target critical infrastructures; generate energy shortages; and seek to defeat Taiwan militarily before the United States could provide effective support. The potential for such harms substantially increases the importance of resilient responses by Taiwan.

The report recommends four major sets of actions to enhance Taiwan’s resilience:

1. Establish a comprehensive security strategy that engages government, the private sector, and individuals in cooperative efforts to ensure all facets of resilience including:
 - a. Risk analyses and priority requirements.
 - b. Organization of data relevant to responding to challenges from the PRC.
 - c. Development of expertise in key areas required for response.
 - d. Provision of governmental leadership and activation of the whole nation as part of a comprehensive approach.

2. Enhance cybersecurity by establishing:
 - a. Off-island, cloud-based capabilities to duplicate governmental and other critical functions.
 - b. Working arrangements with high-end, private-sector cybersecurity providers.
 - c. A surge capability of cybersecurity experts.
 - d. Regular engagement with US Cyber Command’s Hunt Forward program.

Alternatives to undersea cables through low-earth orbit (LEO) communications satellites.

3. Bolster energy security resilience by:
 - a. Rationalizing—that is, increasing—energy prices, especially for electricity.
 - b. Supporting indigenous supply, including nuclear energy.
 - c. Prioritizing energy needs.
 - d. Dispersing and hardening energy storage facilities.
 - e. Preparing comprehensive rationing plans for energy.
4. Enhance defense resilience by:
 - a. Continuing the trend of higher defense spending to at least 3 percent of gross domestic product (GDP).
 - b. Leveraging Taiwan’s strength in high tech manufacturing and shipbuilding to accelerate the development of a Ukraine-style, public-private “capability accelerator”³ for emerging technologies.
 - c. Fielding low-cost, high-effectiveness capabilities including unmanned surface vessels, unmanned aerial vehicles, and naval mines.
 - d. Incorporating training in emerging technologies and unconventional tactics for conscripts and reserves.
 - e. Investing in East Coast port infrastructure as counterblockade strongholds.
 - f. Raising the All-out Defense Mobilization Agency (ADMA) to the national level and implementing a larger civil defense force that fully integrates civilian agencies and local governments.

1 “The gray zone describes a set of activities that occur between peace (or cooperation) and war (or armed conflict),” writes Clementine Starling. “A multitude of activities fall into this murky in-between—from nefarious economic activities, influence operations, and cyberattacks to mercenary operations, assassinations, and disinformation campaigns. Generally, gray-zone activities are considered gradualist campaigns by state and non-state actors that combine non-military and quasi-military tools and fall below the threshold of armed conflict. They aim to thwart, destabilize, weaken, or attack an adversary, and they are often tailored toward the vulnerabilities of the target state. While gray-zone activities are nothing new, the onset of new technologies has provided states with more tools to operate and avoid clear categorization, attribution, and detection—all of which complicates the United States’ and its allies’ ability to respond.” Starling, “Today’s Wars Are Fought in the ‘Gray Zone.’ Here’s Everything You Need to Know About it,” Atlantic Council, February 23, 2022, <https://www.atlanticcouncil.org/blogs/new-atlanticist/todays-wars-are-fought-in-the-gray-zone-heres-everything-you-need-to-know-about-it/>.

2 In a quarantine of Taiwan, Beijing would interdict shipments but allow some supplies—potentially food and medicine—to pass through unimpeded. This measure would enable the PRC to assert greater sovereignty over Taiwan without formally committing to either a war or a blockade.

3 Mykhaylo Lopatin, “Bind Ukraine’s Military-Technology Revolution to Rapid Capability Development,” *War on the Rocks*, January 23, 2024, <https://warontherocks.com/2024/01/bind-ukraines-military-technology-revolution-to-rapid-capability-development/>.

Establish a Comprehensive Security Strategy

Resilience is not a new theme in Taiwan. Former President Tsai Ing-wen, who completed two terms in office on May 20, entitled her 2022 National Day Address “Island of Resilience,”⁴ and similarly identified resilience as a key factor for Taiwan in her two subsequent National Day addresses.⁵ “The work of making the Republic of China (Taiwan) a more resilient country is now our most important national development priority,” she stated in that 2022 speech, in which she articulated four key areas of resilience: economy and industry, social safety net, free and democratic government system, and national defense. What is left undone, however, is aligning these and other resilience elements into a comprehensive security strategy similar to those undertaken by Finland⁶ and Sweden,⁷ which utilize a whole-of society approach to enhance resilience.

Resilience is a nation’s ability to understand, address, respond to, and recover from any type of national security risk. Given the scale of risk Taiwan faces from China, domestic resilience should be front and center in Taiwan’s national security strategy.⁸ Comparable comprehensive national security approaches, such as the Finnish model, aim to foster and enable an engaged national ecosystem of partners, each with a clear understanding of their roles and responsibilities. Finland’s model is instructive, underscoring the importance of engagement by the entire society:

The Security Strategy for Society lays out the general principles governing preparedness in Finnish society. The preparedness is based on the principle of comprehensive security in which the vital functions of society are jointly safeguarded by the authorities, business operators, organisations and citizens.⁹

Comprehensive security thus is far more than just government activities:

Comprehensive security has evolved into a cooperation model in which actors share and analyse security information, prepare joint plans, as well as train and work together. The cooperation model covers all relevant actors, from citizens to the authorities. The cooperation is based on statutory tasks, cooperation agreements and the Security Strategy for Society.¹⁰

The Finnish strategy identifies seven “vital functions” as key areas: leadership; international and European Union activities; defense capability; internal security; economy, infrastructure, and security of supply; functional capacity of the population and services; and psychological resilience.¹¹

Taiwan has taken a variety of actions to enhance resilience including the establishment in 2022 of the All-out Defense Mobilization Agency.¹² That agency has a useful but limited scope with its mandate of “comprehensive management of ‘planning for mobilization, management, service, civil defense, [and] building reserve capacity.’”¹³ But while defense is important (and further discussed below), as the Finnish and Swedish strategies underscore, Taiwan should expand its approach to resilience to include the full spectrum of governmental, private sector, and individual tasks—and the necessary cooperative efforts to make them most effective.

President Lai’s recent election ushered in an unprecedented third consecutive term for the Democratic Progressive Party.¹⁴ This outcome not only provides continuity in the

4 “President Tsai Delivers 2022 National Day Address,” Office of the President of Taiwan, October 10, 2022, <https://english.president.gov.tw/News/6348>.

5 “Full Text of President Tsai Ing-Wen’s National Day Address,” Focus Taiwan website, Central News Agency of Taiwan, October 10, 2023, <https://focustaiwan.tw/politics/202310100004>; and “President Tsai Delivers 2024 New Year’s Address,” Office of the President, Taiwan, January 1, 2024, <https://english.president.gov.tw/NEWS/6662>.

6 Finnish Security Committee, *Security Strategy for Society: Government Resolution*, Ministry of Defense, November 2, 2017, https://turvallisuuskomitea.fi/wp-content/uploads/2018/04/YTS_2017_english.pdf.

7 “Swedish Defence Commission Submits Total Defence Report,” Ministry of Defense, December 19, 2023, <https://www.government.se/articles/2023/12/swedish-defence-commission-submits-total-defence-report/>.

8 Pursuing a professional and structured approach to resilience against Chinese aggression will also have a “halo” effect, building approaches and expertise that will support effective work on other areas of national security risk.

9 Finnish Security Committee, *Security Strategy for Society*.

10 Finnish Security Committee, *Security Strategy for Society*.

11 Finnish Security Committee, *Security Strategy for Society*.

12 “All-out Defense Mobilization Agency,” agency website, n.d., <https://aodm.mnd.gov.tw/aodm-en/indexE.aspx>.

13 John Dotson, “Taiwan’s ‘Military Force Restructuring Plan’ and the Extension of Conscripted Military Service,” Global Taiwan Institute’s *Global Taiwan Brief* 8, no. 3 (2023), <https://globaltaiwan.org/2023/02/taiwan-military-force-restructuring-plan-and-the-extension-of-conscripted-military-service/>.

14 The party does face, however, the governance challenges that come with a hung parliament.

agenda set by the island’s duly elected leader, but also presents an opportunity to sharpen the focus areas for resilience. As Taiwan transitions to a Lai presidency, the challenge of shoring up the island’s resilience should be at the forefront.

As a valuable starting point for establishing such an expanded resilience strategy, the Lai government should undertake extensive consultations with both Finland and Sweden—which could be facilitated as necessary by the United States. Taiwan should also seek to engage with the Hybrid Center of Excellence, based in Finland, which is an “autonomous, network-based international organization countering hybrid threats.”¹⁵

The discussion below describes several important elements of a comprehensive resilience strategy, and it will be a crucial task for the Lai administration to expand Taiwan’s current efforts to the full scope of such an approach. Resilience is a team game with the whole of society playing a role. But only Taiwan’s central government can act as the team captain, setting expectations, establishing priorities, formulating and communicating national strategy, and coordinating activities. Only leaders in national-level government can oversee the critical work of developing institutional effectiveness in key areas of risk management and resilience.

As a starting point, Taiwan should undertake a comprehensive audit now to uncover any gaps in the country’s ability to understand, respond to, and recover from both the chronic risks it currently faces and any more acute manifestations of PRC aggression in the future. Taiwan’s government should examine the following areas to pursue greater resilience:

1. **Activating the whole nation:** Working with the private sector and local government, and communicating to households are essential to develop a truly comprehensive approach to Taiwan’s resilience.
2. **Understanding risk:** Developing a set of scenarios that will help prioritize activities across government and beyond. Prioritizing is critical where resources are limited—as is identifying areas of cross-cutting work that can help to reduce risk in multiple scenarios.
3. **Building data capacity:** Laying a foundation for data exploitation needs will be critical for Taiwan,

which will need this capacity both ahead of and during any crisis response. Preparing for and providing this capacity is not just the preserve of government, as commercially available and industry data sources will provide critical insights. Planning to access, receive, store, and process this data needs to start early, as the foundations for technical infrastructure, capabilities, data-sharing policies, and data expertise in government all require time and cannot just be activated on the cusp of crisis. Part of this work entails developing scenarios to help analysts map out gaps in information sources (intelligence, open source, commercial, and from allies) that Taiwan will likely need in each circumstance to build situational awareness. Ahead of and during crisis, risk assessment and effective decision-making will be highly dependent on the availability, quality, and usability of intelligence, information, and data.

4. **Expanding its network of professional skills and resources:** Assessing the range of skills and the levels of resourcing needed in government to manage a long-term crisis posture should start well ahead of any crisis. It would be helpful to look now at the gaps in key areas of professional expertise: analysts, data experts, crisis-response professionals, and operational planners will all be needed in larger numbers to sustain an effective response. Taiwan will also need professionally administered and well-exercised crisis facilities, resilient technical infrastructure, and business continuity approaches in place.
5. **Preparedness and planning:** Thinking through potential impacts of crisis scenarios in advance and working up potential policy and operational responses will bolster the quality of adaptability, which is an essential component of resilience. The process of exercising and refining plans is also helpful to build the professional connections and networks that will be activated during a live response.

Working with countries that are already developing vanguard resilience capabilities could help Taiwan quickly establish a workable model. For example, the United Kingdom’s National Situation Centre¹⁶—built in less than a year during the COVID-19 pandemic—is a model of developing access to critical data in peacetime and lessons learned from previous crisis scenarios about the practical

15 “Hybrid CoE,” European Centre of Excellence for Countering Hybrid Threats, n.d., <https://www.hybridcoe.fi/>.

16 Lucy Fisher, “First Glimpse Inside UK’s New White House-Style Crisis Situation Centre,” *Telegraph*, December 14, 2021, <https://www.telegraph.co.uk/news/2021/12/14/first-glimpse-inside-uks-new-white-house-style-crisis-situation/>.

challenges a nation could face in a variety of scenarios. Many commercial providers offer competent ways of displaying data insights on dashboards, and while this is helpful, it is only part of what can be achieved.

As a model for its broader resilience requirements, Taiwan will have the benefit of its existing efforts including in the counterdisinformation arena, where it has programs as effective as any in the world, despite the fact that Taiwan consistently faces the world's highest volume of targeted disinformation campaigns.¹⁷ The saturation of PRC information manipulation across Taiwan's traditional and social media platforms is strategically designed to undermine social cohesion, erode trust in government institutions, and soften resistance to Beijing's forced unification agenda, while sowing doubts about America's commitment to peace and stability in the region.

Taiwan has developed a multifaceted strategy to combat this onslaught, eschewing heavy-handed censorship in favor of promoting free speech and empowering civil society. This approach serves as a beacon for other democracies, demonstrating how to effectively counter disinformation through rapid-response mechanisms,

independent fact-checking, along with widespread media literacy initiatives. Collaborative efforts such as the Taiwan FactCheck Center, Cofacts, and MyGoPen have proven instrumental in swiftly identifying and debunking false rumors, notably during the closely watched presidential election on January 13.¹⁸

Taiwan's Minister of Digital Affairs (MoDA) attributes the island's success in combating this "infodemic" to its sophisticated civil-sector efforts, which avoids reliance on reactive takedowns of malicious content akin to a game of whack-a-mole. Much like its handling of the pandemic—where Taiwan achieved one of the world's lowest COVID-19 fatality rates without resorting to draconian lockdowns—it has demonstrated resilience and innovation in the digital sphere.¹⁹

Taiwan's response to disinformation demonstrates that it is well-positioned to establish a comprehensive approach to societal resilience. The discussion below describes several important elements of a comprehensive resilience strategy, but it will be a crucial task for the Lai administration to expand Taiwan's current efforts to the full scope of such an approach.

17 A. Rauchfleisch et al., "Taiwan's Public Discourse About Disinformation: The Role of Journalism, Academia, and Politics," *Journalism Practice* 17, no. 10 (2023): 2197–2217, <https://doi.org/10.1080/17512786.2022.2110928>.

18 Chee-Hann Wu, "Three Musketeers against MIS/Disinformation: Assessing Citizen-Led Fact-Checking Practices in Taiwan," *Taiwan Insight* magazine, July 21, 2023, <https://taiwaninsight.org/2023/03/31/three-musketeers-against-mis-disinformation-assessing-citizen-led-fact-checking-practices-in-taiwan/>; and David Klepper and Huizhong Wu, "How Taiwan Beat Back Disinformation and Preserved the Integrity of Its Election," Associated Press, January 29, 2024, <https://apnews.com/article/taiwan-election-china-disinformation-vote-fraud-4968ef08fd13821e359b8e195b12919c>.

19 E. Glen Weyl and Audrey Tang, "The Life of a Digital Democracy," Plurality (open-source project on collaborative technology and democracy), accessed May 6, 2024, <https://www.plurality.net/v/chapters/2-2/eng/?mode=dark>.

Cybersecurity and critical infrastructure resilience

Cyber risks to critical infrastructures

Like all advanced economies, Taiwan depends on its critical infrastructures. Critical infrastructures have been described as “sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital . . . that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety.”²⁰ Since several critical infrastructures are interlinked, it is important in evaluating resilience to “capture cross-cutting risks and associated dependencies that may have cascading impacts within and across sectors.”²¹ Among those interlinked critical infrastructures are energy, communications, transportation, and water. Each of these are critical to society as a whole and each are dependent on digital technology for their operations.

In Taiwan, the Administration for Cyber Security has identified critical infrastructures “by their feature types into the following eight fields: energy, water resource, telecommunications, transportation, banking and finance, emergency aid and hospitals, central and local governments, and high-tech parks.”²² It is worth underscoring that several of Taiwan’s critical infrastructures, such as the electric grid²³ and the water system,²⁴ are significantly centralized or have other notable vulnerabilities such as the dependency on undersea cables for international communications²⁵ that increase the potential consequences from a successful cyberattack.

The Taiwan government has fully recognized the significant risks from cyberattacks. As described by Taiwan’s Administration for Cyber Security, “Due to Taiwan’s unique political and economic situation, the country faces not only a complex global cyber security environment but also severe cyber security threats, making the continuous implementation and improvement of cyber security measures a necessity.”²⁶

The number of cyberattacks against Taiwan is notable.²⁷ Published estimates range from five million cyberattacks per day against Taiwanese government agencies²⁸ to the detection of 15,000 cyberattacks per second, including attempted intrusions, in Taiwan during the first half of 2023.²⁹

The attacks often focus on key societal infrastructures. A recent Voice of America report noted that just prior to the January 2024 elections:

Most of the attacks appeared to focus on government offices, police departments, and financial institutions, with the attackers focused on internal communications, police reports, bank statements and insurance information.³⁰

Google researchers have likewise described the cyber threat to key critical infrastructures, revealing that it is “tracking close to 100 hacking groups out of China [and that these] malicious groups are attacking a wide spectrum

20 “Critical Infrastructure Sectors,” US Cybersecurity and Infrastructure Security Agency (CISA), 2022, <https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors>.

21 “National Critical Functions,” CISA, n.d., <https://www.cisa.gov/topics/risk-management/national-critical-functions>.

22 Taiwan Administration for Cyber Security, “Cyber Security Defense of Critical Infrastructure: Operations,” Ministry of Digital Affairs, February 21, 2023, <https://moda.gov.tw/en/ACS/operations/ciip/650>.

23 “Taipower Announces Grid Resilience Strengthening Construction Plan with NT\$564.5 Billion Investment Over 10 Years, Preventing Recurrence of Massive Power Outages,” Ministry of Economic Affairs, September 15, 2022, https://www.moea.gov.tw/MNS/english/news/News.aspx?kind=6&menu_id=176&news_id=103225#:~:text=Wen%2DSheng%20Tseng%20explained%20that,of%20electricity%20demand%20in%20Taiwan.

24 Taiwan Water Corporation provides most of the water in Taiwan. See Taiwan Water Corporation, <https://www.water.gov.tw/en>.

25 Wen Lii, “After Chinese Vessels Cut Matsu Internet Cables, Taiwan Seeks to Improve Its Communications Resilience,” Opinion, *Diplomat*, April 15, 2023, <https://thediplomat.com/2023/04/after-chinese-vessels-cut-matsu-internet-cables-taiwan-shows-its-communications-resilience/>.

26 “About Us: History,” Administration for Cyber Security, MoDA, n.d., <https://moda.gov.tw/en/ACS/aboutus/history/608>. Note: US government analyses likewise underscore the significant number of attacks. As described by the US International Trade Administration (ITA), “Taiwan faces a disproportionately high number of cyberattacks, receiving as many as 30 million attacks per month in 2022.” See “Taiwan—Country Commercial Guide,” US ITA, last published January 10, 2024, <https://www.trade.gov/country-commercial-guides/taiwan-cybersecurity>.

27 Statistics are not entirely consistent, and attempted intrusions are sometimes counted as attacks.

28 “Taiwanese Gov’t Facing 5M Cyber Attacks per Day,” *CyberTalk*, Check Point Software Technologies, accessed May 2, 2024, <https://www.cybertalk.org/taiwanese-govt-facing-5m-cyber-attacks-per-day/>. Other private-sector companies’ analyses have reached comparable conclusions.

29 Huang Tzu-ti, “Taiwan Hit by 15,000 Cyberattacks per Second in First Half of 2023,” *Taiwan News*, August 17, 2023, <https://www.taiwannews.com.tw/news/4973448>.

30 Jeff Seldin, “Cyber Attacks Spike Suddenly prior to Taiwan’s Election,” Voice of America, February 13, 2024, <https://www.voanews.com/a/cyber-attacks-spike-suddenly-prior-to-taiwan-s-election-/7485386.html>.

of organizations, including the government, private industry players and defense organizations.”³¹

The attacks themselves are often relatively sophisticated. Trellix, a cybersecurity firm, described multiple techniques utilized by attackers that “focused on defense evasion, discovery, and command and control . . . to subvert system defenses to gather information about accounts, systems, and networks.” Among them are “living-off-the-land” techniques, which allow attackers to maintain their intrusions over time with smaller chances of detection.³²

While no one can say with certainty what actions the PRC would take in the context of a blockade of or outright conflict with Taiwan, the United States is clear-eyed about the potential for attacks on its own critical infrastructures if engaged in conflict with China. The February 2023 *Annual Threat Assessment of the US Intelligence Community* notes the likelihood of such PRC cyberattacks in that context:

If Beijing feared that a major conflict with the United States were imminent, it almost certainly would consider undertaking aggressive cyber operations against U.S. homeland critical infrastructure and military assets worldwide . . . China almost certainly is capable of launching cyber attacks that could disrupt critical infrastructure services within the United States, including against oil and gas pipelines, and rail systems.³³

The ongoing Russian cyberattacks against Ukraine in the Russia-Ukraine war further underscore the reality of critical infrastructures as a target in a conflict. It seems reasonable to assume that comparable actions (and perhaps even more) would be undertaken against Taiwan in the event of a blockade or kinetic conflict. “Probable targets,” according to James A. Lewis, would include critical infrastructures such as electrical power facilities, information and communications systems, and pipelines.³⁴

Actions to enhance Taiwan’s cyber resilience

Taiwan can enhance its cyber resilience through its own actions and in collaborative activities with private-sector companies and with the United States. While cyberattacks can be highly disruptive, one of the important lessons of the Ukraine-Russia conflict is that the effects on operations can be mitigated, as described in a CyberScoop analysis that underscores a shift in expectations:

The war has inspired a defensive effort that government officials and technology executives describe as unprecedented—challenging the adage in cybersecurity that if you give a well-resourced attacker enough time, they will pretty much always succeed. The relative success of the defensive effort in Ukraine is beginning to change the calculation about what a robust cyber defense might look like going forward.³⁵

According to the analysis, the critical element for such success has been significant multinational and public-private collaboration:

This high level of defense capability is a consequence of a combination of Ukraine’s own effectiveness, significant support from other nations including the United States and the United Kingdom, and a key role for private sector companies.

The defensive cyber strategy in Ukraine has been an international effort, bringing together some of the biggest technology companies in the world such as Google and Microsoft, Western allies such as the U.S. and Britain and social media giants such as Meta who have worked together against Russia’s digital aggression.³⁶

31 Gagandeep Kaur, “Is China Waging a Cyber War with Taiwan?,” CSO Online, December 1, 2023, <https://www.csoonline.com/article/1250513/is-china-waging-a-cyber-war-with-taiwan.html#:~:text=Nation%2Dstate%20hacking%20groups%20based>.

32 Anne An wrote that “attackers are likely to employ living off-the-land techniques to gather policing, banking, and political information to achieve their goals. They also likely simultaneously and stealthily evaded security detections from remote endpoints.” See An, “Cyberattack on Democracy: Escalating Cyber Threats Immediately Ahead of Taiwan’s 2024 Presidential Election,” Trellix, February 13, 2024, <https://www.trellix.com/blogs/research/cyberattack-on-democracy-escalating-cyber-threats-immediately-ahead-of-taiwan-2024-presidential-election/>. Separately, a Microsoft *Threat Intelligence* blog said: “Microsoft has identified a nation-state activity group tracked as Flax Typhoon, based in China, that is targeting dozens of organizations in Taiwan with the likely intention of performing espionage. Flax Typhoon gains and maintains long-term access to Taiwanese organizations’ networks with minimal use of malware, relying on tools built into the operating system, along with some normally benign software to quietly remain in these networks.” See “Flax Typhoon Using Legitimate Software to Quietly Access Taiwanese Organizations,” Microsoft *Threat Intelligence* blog, August 24, 2023, <https://www.microsoft.com/en-us/security/blog/2023/08/24/flax-typhoon-using-legitimate-software-to-quietly-access-taiwanese-organizations/>.

33 Office of the Director of National Intelligence, *Annual Threat Assessment of the US Intelligence Community*, February 6, 2023, 10, <https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf>.

34 James Lewis, “Cyberattack on Civilian Critical Infrastructures in a Taiwan Scenario,” Center for Strategic and International Studies, August 2023, https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-08/230811_Lewis_Cyberattack_Taiwan.pdf?VersionId=l.gf7ysPjoW3.OcHvcRuNcpq3gN.Vj8b.

35 Elias Groll and Aj Vicens, “A Year After Russia’s Invasion, the Scope of Cyberwar in Ukraine Comes into Focus,” CyberScoop, February 24, 2023, <https://cyberscoop.com/ukraine-russia-cyberwar-anniversary/>.

36 Groll and Vicens, “A Year After Russia’s Invasion.”

Actions by Taiwan

Taiwan should utilize the Ukraine model of cyber resilience—backed in part by private-sector companies—and take comparable actions to enhance its cybersecurity. Taiwan has a substantial existing cybersecurity framework on which to build such mitigating actions. Since 2022, the Ministry of Digital Affairs, through its Administration for Cyber Security, is responsible for “implementing cyber security management and defense mechanisms for national critical infrastructures” including “evaluating and auditing cyber security works at government agencies and public entities.”³⁷ Utilizing that framework, Taiwan should undertake the following four actions that would significantly enhance the island’s cybersecurity resilience.

First, Taiwan should utilize cloud-based capabilities to establish a duplicative set of cyber-enabled governmental functions outside of Taiwan. Ukraine undertook such actions, thereby rendering Russian cyberattacks in Ukraine unable to disrupt ongoing governmental activities. Taiwan’s Ministry of Digital Affairs has been evaluating the use of public clouds including the possibility of “digital embassies” abroad to hold data.³⁸ Taiwan should organize such actions with key cloud providers such as Amazon Web Services, which provided support to Ukraine.³⁹ The United States should work with Taiwan and appropriate cloud providers to help effectuate such a result.

Second, Taiwan should establish arrangements with private-sector cybersecurity providers to undertake defensive operations against PRC cyberattacks in the context of a blockade or kinetic conflict. As noted above, such private-sector actions have been instrumental to Ukraine, and would similarly be invaluable for Taiwan. The United States should also help facilitate such private-sector defensive cyber operations for Taiwan.

Third, Taiwan should organize a surge capability of individual cybersecurity experts who can be called upon to complement governmental resources. Both Estonia and the United Kingdom have very effective cyber-reserve approaches, and Taiwan should engage with each country,

seeking lessons learned as part of establishing its own reserve corps.

Fourth, Taiwan needs to accelerate its low-earth orbit satellite communications program. The Ministry of Digital Affairs’ two-year, US\$18 million plan to strengthen the resilience of government communications entails building more than 700 satellite receiver stations. The impetus: ships from mainland China have repeatedly severed submarine internet cables in what Taiwan perceived as “a trial of methods” that the PRC could use to prepare for a military invasion.⁴⁰

The existing program involves satellites as well as ground-based receivers. The Taiwan Space Agency disclosed its plan for a “dedicated” LEO satellite communications project in late 2022,⁴¹ as a public-private partnership:

Distinct from traditional government programs, this groundbreaking project is structured as a privately operated venture, wherein the Taiwanese government would retain a substantial minority ownership. . . . This project intends to enhance the Taiwan Space Agency’s initial proposal for two government-built LEO satellites by evolving it into a “2+4” configuration. This will involve constructing four additional satellites through collaborative efforts between the public and private sectors.⁴²

Actions with the United States

In accord with the Taiwan Relations Act,⁴³ and as a matter of long-standing policy, the United States strongly supports Taiwan’s defensive capabilities including for cybersecurity. The Integrated Country Strategy of the American Institute in Taiwan (essentially the unofficial US embassy) specifically provides that “bolster[ing] Taiwan’s cybersecurity resilience” is one of the United States’ strategic priorities for the island.⁴⁴ To support that objective, the United States can enhance Taiwan cybersecurity through cooperative defensive activities.

First, US Cyber Command regularly supports the network resilience of allied countries and partners through its “Hunt

37 “About Us: History,” Administration for Cyber Security.

38 Si Ying Thian, “‘Turning Conflicts into Co-creation’: Taiwan Government Harnesses Digital Policy for Democracy,” *GovInsider*, December 6, 2023, <https://govinsider.asia/intl-en/article/turning-conflicts-into-co-creation-taiwans-digital-ministry-modernization-harnesses-digital-policy-for-democracy>.

39 Frank Konkel, “How a Push to the Cloud Helped a Ukrainian Bank Keep Faith with Customers amid War,” *NextGov/FCW*, November 30, 2023, <https://www.nextgov.com/modernization/2023/11/how-push-cloud-helped-ukrainian-bank-keep-faith-customers-amid-war/392375/>.

40 Eric Priezkalns, “Taiwan to Build 700 Satellite Receivers as Defense against China Cutting Submarine Cables,” *CommsRisk*, June 13, 2023, <https://commsrisk.com/taiwan-to-build-700-satellite-receivers-as-defense-against-china-cutting-submarine-cables/>.

41 Juliana Suess, “Starlink 2.0? Taiwan’s Plan for a Sovereign Satellite Communications System,” *Commentary*, Royal United Services Institute, January 20, 2023, <https://rusi.org/explore-our-research/publications/commentary/starlink-20-taiwans-plan-sovereign-satellite-communications-system>.

42 Gil Baram, “Securing Taiwan’s Satellite Infrastructure against China’s Reach,” *Lawfare*, November 14, 2023, <https://www.lawfaremedia.org/article/securing-taiwan-s-satellite-infrastructure-against-china-s-reach>.

43 Taiwan Relations Act, US Pub. L. No. 96-8, 93 Stat. 14 (1979), <https://www.congress.gov/96/statute/STATUTE-93/STATUTE-93-Pg14.pdf>.

44 “Integrated Country Strategy,” American Institute in Taiwan, 2022, https://www.state.gov/wp-content/uploads/2022/05/ICS_EAP_Taiwan_Public.pdf.

Forward” operations, which are “strictly defensive” joint ventures, undertaken following an invitation from the ally or partner, to “observe and detect malicious cyber activity” on these networks, together searching out “vulnerabilities, malware, and adversary presence.”⁴⁵

While Taiwan has not been specifically identified as a Hunt Forward participant, Anne Neuberger, who is the US deputy national security advisor for cyber and emerging technology, said at a Politico Tech Summit in 2023 that in the event of a major cyberattack on Taiwan, the United States would “send its best teams to help hunt down the attackers, the same approach typically used to help global allies in cyberspace.”⁴⁶ She described the typical approach as:

Putting our best teams to hunt on their most sensitive networks to help identify any current intrusions and to help remediate and make those networks as strong as possible.⁴⁷

Neuberger also highlighted US work with Taiwan to carry out military tabletop games and exercises to prepare for potential cyberattack.⁴⁸

More recently, the National Defense Authorization Act (NDAA) for Fiscal Year 2024 explicitly authorized the Defense Department to cooperate on:

Defensive military cybersecurity activities with the military forces of Taiwan to (1) defend military networks, infrastructure, and systems; (2) counter malicious cyber activity that has compromised such military networks, infrastructure, and systems; (3) leverage United States commercial and military cybersecurity technology and services to harden and defend such military networks, infrastructure, and

systems; and (4) conduct combined cybersecurity training activities and exercises.⁴⁹

Going forward, those authorities authorize not only Hunt Forward actions but also actions to leverage commercial and military technology to harden such networks (which would seem to resolve any export control issues) and to conduct combined training and exercises, all of which underscores clear congressional approval for enhanced cybersecurity activities with Taiwan.⁵⁰

Second, the United States should undertake to enhance Taiwan’s communications resilience by making available access to US commercial and military LEO networks. The important role of the commercial provider Starlink in assuring communications in the context of the Ukraine-Russia war is well-known.⁵¹ Starlink’s parent company, SpaceX, is, however, controlled by Elon Musk, whose Tesla company has major investments in China. That linkage has raised the question of whether Taiwan could rely on any commercial arrangements it might make on its own with Starlink—particularly since Starlink did impose some limitations on Ukraine’s use of the network.⁵² However, as previously described by one of the authors of this report, the US government has sway on such matters:

The Defense Production Act authorizes the [US] government to require the prioritized provision of services—which would include services from space companies—and exempts any company receiving such an order from liabilities such as inability to support other customers.⁵³

Accordingly, the US should rely on this authority to organize appropriate arrangements with Starlink—and other space companies that provide like capabilities—to ensure access that would support Taiwan communications.

45 Franklin D. Kramer, *The Sixth Domain: The Role of the Private Sector in Warfare*, Atlantic Council, October 16, 2023, 13, <https://www.atlanticcouncil.org/wp-content/uploads/2023/10/The-sixth-domain-The-role-of-the-private-sector-in-warfare-Oct16.pdf>.

46 Joseph Gedeon, “Taiwan Is Bracing for Chinese Cyberattacks, White House Official Says,” *Politico*, September 27, 2023, <https://www.politico.com/news/2023/09/27/taiwan-chinese-cyberattacks-white-house-00118492>.

47 Gedeon, “Taiwan Is Bracing.”

48 Gedeon, “Taiwan Is Bracing.”

49 National Defense Authorization Act for Fiscal Year 2024, Pub. L. No. 118-31, 137 Stat. 136 (2023), Sec. 1518, <https://www.congress.gov/bill/118th-congress/house-bill/2670/text>.

50 National Defense Authorization Act for Fiscal Year 2024.

51 According to a report by Emma Schroeder and Sean Dack, “Starlink’s performance in the Ukraine conflict demonstrated its high value for wartime satellite communications: Starlink, a network of low-orbit satellites working in constellations operated by SpaceX, relies on satellite receivers no larger than a backpack that are easily installed and transported. Because Russian targeting of cellular towers made communications coverage unreliable . . . the government ‘made a decision to use satellite communication for such emergencies’ from American companies like SpaceX. Starlink has proven more resilient than any other alternatives throughout the war. Due to the low orbit of Starlink satellites, they can broadcast to their receivers at relatively higher power than satellites in higher orbits. There has been little reporting on successful Russian efforts to jam Starlink transmissions.” See Schroeder and Dack, *A Parallel Terrain: Public-Private Defense of the Ukrainian Information Environment*, Atlantic Council, February 2023, 14, <https://www.atlanticcouncil.org/wp-content/uploads/2023/02/A-Parallel-Terrain.pdf>.

52 Joey Roulette, “SpaceX Curbed Ukraine’s Use of Starlink Internet for Drones: Company President,” *Reuters*, February 9, 2023, <https://www.reuters.com/business/aerospace-defense/spacex-curbed-ukraines-use-starlink-internet-drones-company-president-2023-02-09/>.

53 Kramer, *The Sixth Domain*.

One way to do this would be to incorporate appropriate terms into the commercial augmentation space reserve (CASR) program arrangements that US Space Force is currently negotiating with civil space providers,⁵⁴ as part of the Department of Defense’s overall commercial space strategy.⁵⁵

Additionally, the DOD is developing its own LEO capability through a variety of constellations being put in place by Space Force.⁵⁶ Pursuant to the recent NDAA authorization noted above, DOD should work with the Taiwan military to ensure that those constellations will be available to support Taiwan as necessary.

Longer term, the United States should also undertake to enhance the resilience of Taiwan’s undersea cables. As previously proposed by one of the authors, the United States should lead in establishing an international undersea infrastructure protection corps. It should:

Combine governmental and private activities to support the resilience of undersea cables and pipelines. Membership should include the United States, allied nations with undersea maritime capabilities, and key private-sector cable and pipeline companies.⁵⁷

Such an activity would include focus on cybersecurity for undersea cable networks, hardening and other protection for cable landing points, and capabilities and resources to ensure expeditious repair of cables as needed.⁵⁸ To be

sure, getting such an activity up and running will necessarily be a multiyear effort. However, Taiwan’s vulnerability underscores the importance of beginning promptly and working as expeditiously as possible.

Cybersecurity recommendations for Taiwan

- Utilize cloud-based capabilities to establish a duplicative set of cyber-enabled governmental functions outside of Taiwan.
- Establish arrangements with private-sector cybersecurity providers to undertake defensive operations against PRC cyberattacks.
- Organize a surge capability of individual cybersecurity experts who can be called upon to complement governmental resources.
- Accelerate the low-earth orbit satellite communications program.
- Actively engage with Cyber Command’s Hunt Forward activities.
- Enhance Taiwan’s communications resilience by making available access to US commercial and military LEO networks.
- Undertake on a longer-term basis enhanced resilience of Taiwan’s undersea cables.

54 Frank Kramer, Ann Dailey, and Joslyn Brodfuehrer, *NATO Multidomain Operations: Near- and Medium-term Priority Initiatives*, Scowcroft Center for Strategy and Security, Atlantic Council, March 2024, <https://www.atlanticcouncil.org/wp-content/uploads/2024/03/NATO-multidomain-operations-Near-and-medium-term-priority-initiatives.pdf>.

55 Department of Defense, “Commercial Space Integration Strategy,” 2024, <https://media.defense.gov/2024/Apr/02/2003427610/-1/-1/2024-DOD-COMMERCIAL-SPACE-INTEGRATION-STRATEGY.PDF>; and “U.S. Space Force Commercial Space Strategy,” US Space Force, April 8, 2024, https://www.spaceforce.mil/Portals/2/Documents/Space%20Policy/USSF_Commercial_Space_Strategy.pdf.

56 “Space Development Agency Successfully Launches Tranche 0 Satellites,” Space Development Agency, September 2, 2023, <https://www.sda.mil/space-development-agency-completes-second-successful-launch-of-tranche-0-satellites/>.

57 Kramer, *The Sixth Domain*.

58 Kramer, *The Sixth Domain*.

Energy

As part of its efforts to enhance resilience, Taiwan must mitigate its energy vulnerabilities, as its reliance on maritime imports for about 97 percent⁵⁹ of its energy needs creates acute risks. To lessen its dependency on maritime imports and strengthen its resiliency in the face of potential PRC coercion, Taiwan should curb energy and electricity demand, bolster indigenous supply, overhaul its inventory management, and prepare rationing plans. A resilient energy security approach would credibly signal to the PRC that Taiwan could hold out for long durations without maritime resupply.

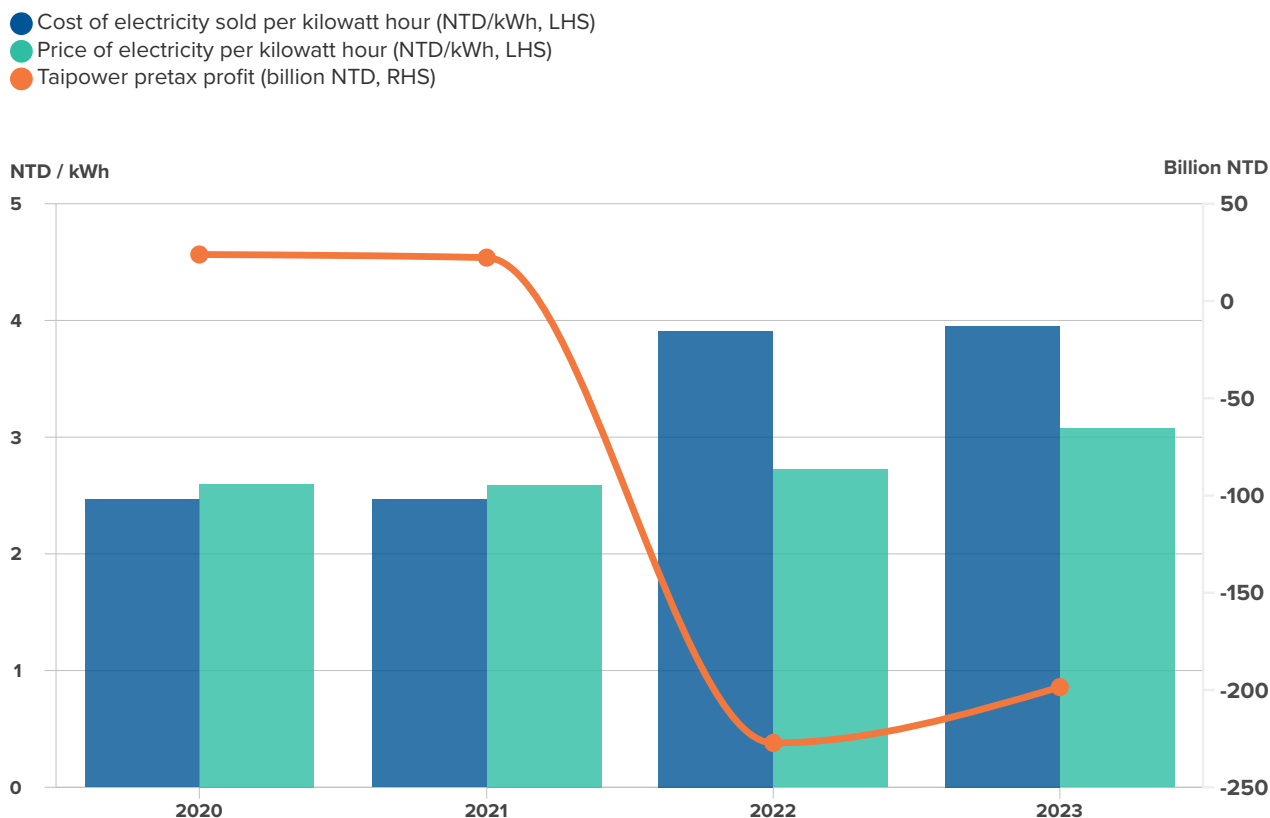
Curbing demand by rationalizing prices

Taiwan’s ultra-low electricity prices are a security risk (and a black eye for its climate targets). Reliance on seaborne

energy shipments presents straightforward security problems, and Taiwan’s low electricity prices subsidize consumption that is being met by imports of hydrocarbons, especially coal. The new Lai administration should make haste prudently, increasing electricity prices more frequently and significantly, without exceeding the limits of the politically possible.

Taiwan’s electricity price quandary is illustrated by Taipower, the state-owned monopoly utility. In 2022 and 2023, Taipower lost 227.2 billion New Taiwan dollars (NTD) and 198.5 billion NTD, respectively, as its per kilowatt hour cost of electricity sold substantially exceeded per unit prices.⁶⁰ Taipower’s prices failed to offset the steep rise in electricity input costs amid Russia’s invasion of Ukraine and the post-COVID-19 unsnarling of supply chains.

Figure 1: Taipower electricity prices and profits

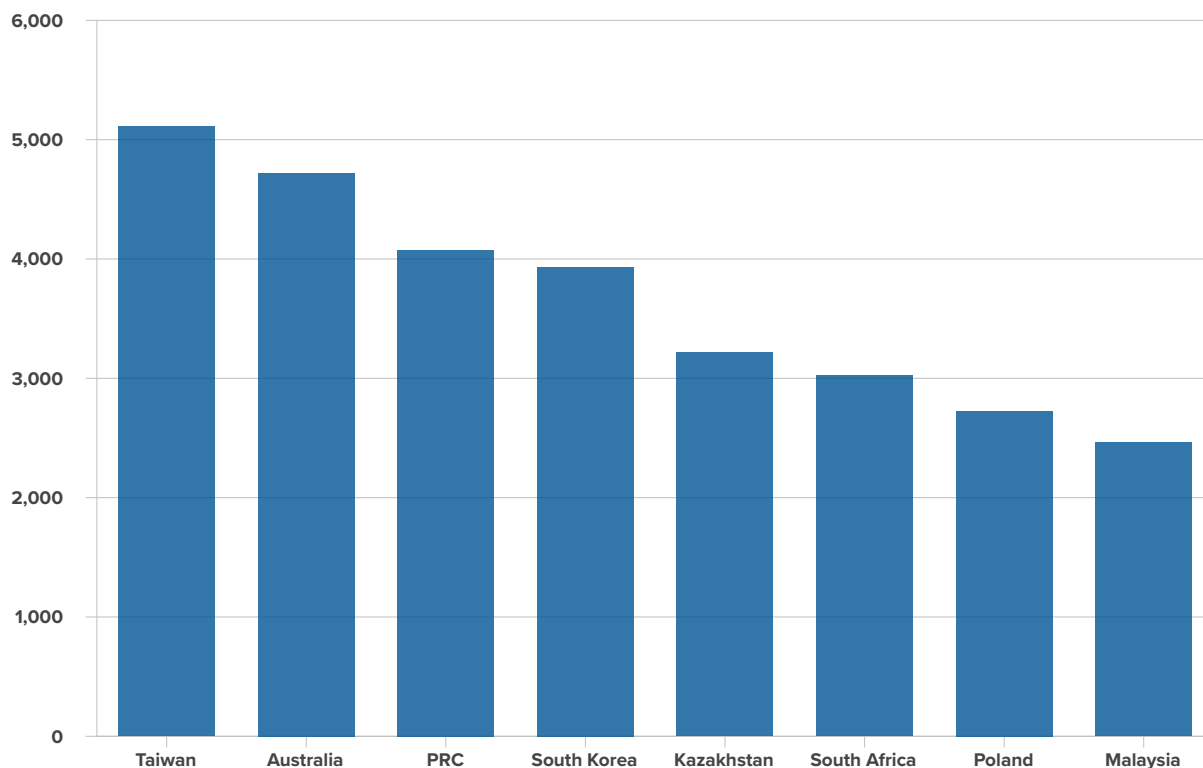


Sources: Authors’ calculations using Taipower.com data. Note: LHS stands for left-hand side; RHS for right-hand side.

59 “E-Stat,” Energy Statistics Monthly Report, Energy Administration, Taiwan Ministry of Economic Affairs, accessed May 6, 2024, <https://www.esist.org.tw/newest/monthly?tab=%E7%B6%9C%E5%90%88%E8%83%BD%E6%BA%90>.

60 “Comparison of Electricity Prices and Unit Cost Structures,” Electricity Price Cost, Business Information, Information Disclosure, Taiwan Electric Power Co., accessed May 6, 2024, <https://www.taipower.com.tw/tc/page.aspx?mid=196>.

Figure 2: Per capita kWh consumption of electricity generation from coal, by economy (2023)



Sources: Authors’ calculations; Energy Institute’s *Statistical Review of World Energy*, <https://www.energyinst.org/statistical-review>; IMF’s World Economic Outlook Database <https://www.imf.org/en/Publications/WEO/weo-database/2024/April>;

Taiwan’s electricity costs remain too low, diminishing the island’s resiliency, although policymakers have now taken some steps in light of the problem. The Ministry of Economic Affairs’ latest electricity price review, in March 2024, raised average prices by about 11 percent, with the new tariff reaching about 3.4518 NTD, or approximately \$0.11 USD/kWh.⁶¹ This rationalization of prices, while welcome, is insufficient. In the United States, the rolling twelve-month ending price in January 2024 for all sectors totaled \$0.127/kWh.⁶² Taiwan’s heavily subsidized electricity consumers therefore enjoy a discount in excess of 13 percent compared to their US counterparts, despite US access to low-cost, abundant, and indigenously produced energy.

Taiwan’s heavily subsidized electricity prices incentivize maritime imports, especially coal. Astonishingly, Taiwan was the world’s largest per capita user of coal generation

for electricity in 2022, higher than even Australia, a major coal exporter.

Taiwan’s low electricity prices and use of coal expose the island to PRC economic coercion. Taiwan’s dependency on imported coal heightens its vulnerability in the summer, when the island’s electricity-generation needs peak. Concerningly, Taiwan has already experienced electricity shortfalls in summer *peacetime* conditions, including a wave of outages⁶³ between July and August 2022. With the island’s future summer cooling needs set to rise even further due to climate change and hotter temperatures, Taiwan’s electricity needs pose a vulnerability that the PRC may attempt to exploit.

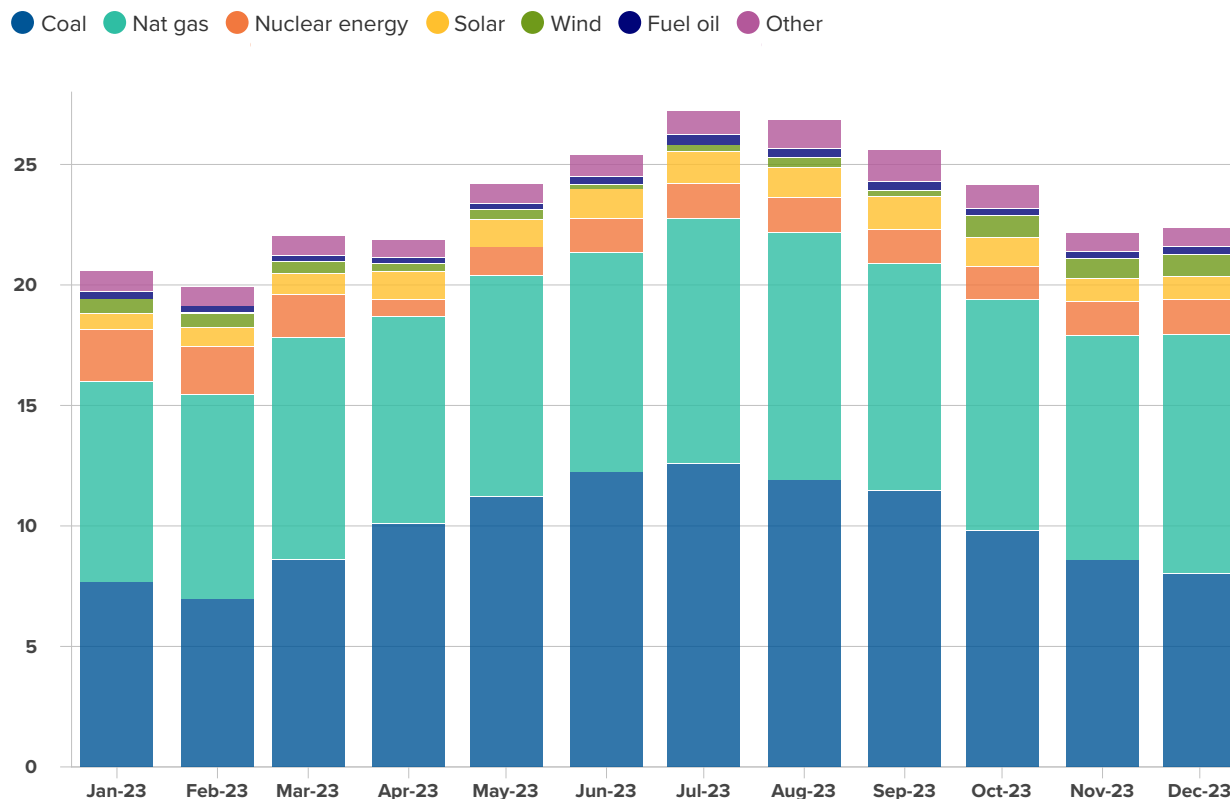
Curbing Taiwan’s electricity demand during summer months is critical, necessitating a rise in prices. While this reduction is a principal energy security challenge, the

61 Ministry of Economic Affairs (經濟部能源署), “The Electricity Price Review Meeting,” Headquarters News, accessed May 6, 2024, https://www.moea.gov.tw/MNS/populace/news/News.aspx?kind=1&menu_id=40&news_id=114222.

62 “Electric Power Monthly,” US Energy Information Administration (EIA), February 2024, https://www.eia.gov/electricity/monthly/epm_table_grapher.php?t=table_5_03.

63 Lauly Li and Cheng Ting-Feng, “Taiwan’s Frequent Blackouts Expose Vulnerability of Tech Economy,” *Nikkei Asia*, August 30, 2022, <https://asia.nikkei.com/Business/Technology/Taiwan-s-frequent-blackouts-expose-vulnerability-of-tech-economy>.

Figure 3: Taiwan seasonal electricity generation, 2023
(Terawatt hours)



Sources: Authors' calculations; Energy Administration, Ministry of Economic Affairs, "Power Generation (發電量)," database accessed May 6, 2024.

island must also do more to secure supply, especially for nuclear energy.

Supply: Support indigenous production

Taiwan's resiliency will be strengthened by producing as much indigenous energy as possible, especially during the critical summer months. Taiwan, which has virtually no hydrocarbon resources, can therefore indigenously produce only four different forms of energy at scale: nuclear energy, offshore wind, onshore wind, and solar. Taiwan should pursue each of these indigenous energy sources. Taiwan should apply "carrots" by strengthening incentives and payments for indigenous production. At the same time, applying the "stick" of higher prices to energy consumption, especially for energy imports, would bolster the island's resiliency.

Taiwan's renewable resources are significant and often economically viable, but they cannot secure adequate levels of resiliency by themselves. Taiwan's wind speeds slow in the summer,⁶⁴ limiting onshore and offshore wind's effectiveness in bolstering energy security. Additionally, Taiwan's stringent localization requirements for offshore appropriately minimize PRC components and sensors in Taiwan's offshore wind turbines, but also raise the costs of this technology. Taiwan's solar potential⁶⁵ is also limited⁶⁶ by cloudy skies, frequent rainfall, and land scarcity.

Accordingly, nuclear energy is the most viable way for Taiwan to address its summer electricity needs without turning to maritime imports. While Taiwan's nuclear reactors must acquire fuel from abroad, this fuel can be used for approximately eighteen to twenty-four months.⁶⁷ Taiwan should maintain its existing nuclear energy capacity; restart

64 Xi Deng et al., "Offshore Wind Power in China: A Potential Solution to Electricity Transformation and Carbon Neutrality," *Fundamental Research*, 2022, <https://doi.org/10.1016/j.fmre.2022.11.008>.

65 "Global Solar Atlas," World Bank Group, ESMAP, and Solar GIS, 2024, CC BY 4.0, <https://globalsolaratlas.info/map?c=24.176825>.

66 Julian Spector, "Taiwan's Rapid Renewables Push Has Created a Bustling Battery Market," *Canary Media*, April 6, 2023, <https://www.canarymedia.com/articles/energy-storage/taiwans-rapid-renewables-push-has-created-a-bustling-battery-market>.

67 "U.S. Nuclear Plant Outages Increased in September After Remaining Low during Summer," *Today in Energy*, US EIA, October 18, 2015, <https://www.eia.gov/todayinenergy/detail.php?id=37252#:~:text=Nuclear%20power%20plants%20typically%20refuel>.

retired capacity as soon as politically and technically feasible; and seek new, incremental capacity over time.⁶⁸

Unpacking Taiwan's storage complexities: Dispersal and hardening is critical

To cope with various contingencies, including the possibility of a prolonged summertime blockade, Taiwan should increase its stockpiles of energy, disperse inventory around the island, and harden facilities.

While Taiwan's ability to hold out against a blockade involves by many factors, energy inventories are a critical element. Taiwan's electricity reserves are limited: it reported fifty-six days of supply of coal inventories in February 2023,⁶⁹ and aims to raise its natural gas inventories from eleven days to more than twenty days by 2030.⁷⁰ These inventory levels should be expanded, in part because "days of supply" fail to encapsulate uncertainty. Demand fluctuates depending on temperature and other variables, while Taiwan's access to energy storage inventories faces the risk of sabotage and, in certain scenarios, kinetic strikes.

Taiwan's management of petroleum reserves is a matter of great importance, given the use of these fuels, especially diesel, for military matters. Taiwan's Energy Administration, in the Ministry of Economic Affairs, reported in April 2024 that its total oil inventories stood at 167 days of supply.⁷¹ This topline figure presents an overly optimistic portrait of Taiwan's petroleum security, however. For instance, Taiwan's government-controlled inventories in April 2024⁷² included 2.6 million kiloliters of crude oil and refined products; private stocks added another 6.5 million kiloliters. Accordingly, Taiwan reports forty-seven days of supply from government stockpiles, with an additional 120 days from private inventories.⁷³ Given that domestic sales and consumption equated to about 54,200 kiloliters per day from prior comparable periods,⁷⁴ Taiwan calculated it had about 167 days of supply.

There may, however, be insufficient monitoring of private inventories. Marek Jestrab observed:

A concerning—and possibly significant—loophole exists in these laws, where the criteria and computation formulas for the actual on-hand security stockpiles will be determined by the central competent authority, and are not required to be disclosed. This presents the opportunity for energy that is loaded onboard merchant shipping while in transit to Taiwan to count toward these figures.⁷⁵

While Taiwan should ensure that stockpiles are actually on the island, and not at sea, it also needs to carefully examine the inventory split between crude oil and crude products, such as diesel, gasoline, jet fuel, etc. Additionally, Taiwan's policymakers should not expect to rely on its crude inventories, which only have a latent potential: crude oil cannot be used until it is refined into a crude product. Therefore, if the PRC disrupted Taiwan's refineries via cyber or even kinetic means, Taiwan would not be able to access the totality of its crude oil reserves.

Taiwan's military requirements for fuel would likely surge during a confrontation or conflict with the PRC, reducing the "days of supply." Since Taiwan's military vehicles largely run on diesel, the island should pay careful attention to this product.

Taiwan should disperse and harden its energy assets, especially diesel storage, as concentrated objects would present inviting targets for the PRC. Beijing is studying Russia's invasion of Ukraine closely and will not fail to notice that Moscow attacked about 30 percent of Ukrainian infrastructure in a single day.⁷⁶ As one author witnessed during his recent visit to Kyiv, Ukraine's dispersal of electricity assets is achieving a reasonable degree of success. Indeed, Russia's more

68 For a more detailed discussion of Taiwan's indigenous supply, see Joseph Webster, "Does Taiwan's Massive Reliance on Energy Imports Put Its Security at Risk?," *New Atlanticist*, Atlantic Council blog, July 7, 2023, <https://www.atlanticcouncil.org/blogs/new-atlanticist/does-taiwans-massive-reliance-on-energy-imports-put-its-security-at-risk/>.

69 "The Current Situation and Future of [the] Country's Energy Supply and Reserves (立法院)," Seventh Session of the Tenth Legislative Yuan, Sixth Plenary Meeting of the Economic Committee, accessed May 7, 2024, <https://ppg.ly.gov.tw/ppg/SittingAttachment/download/2023030989/02291301002301567002.pdf>.

70 Jeanny Kao and Yimou Lee, "Taiwan to Boost Energy Inventories amid China Threat," ed. Gerry Doyle, Reuters, October 23, 2022, <https://www.reuters.com/business/energy/taiwan-boost-energy-inventories-amid-china-threat-2022-10-24/>.

71 Energy Administration, "Domestic Oil Reserves Monthly Data (國內石油安全存量月資料)," Ministry of Economic Affairs, accessed May 6, 2024, https://www.moeaea.gov.tw/ecw/populace/content/wfrmStatistics.aspx?type=4&menu_id=1302.

72 Energy Administration, Ministry of Economic Affairs.

73 Energy Administration, Ministry of Economic Affairs.

74 Energy Administration, Ministry of Economic Affairs.

75 Marek Jestrab, "A Maritime Blockade of Taiwan by the People's Republic of China: A Strategy to Defeat Fear and Coercion," Atlantic Council Strategy Paper, December 12, 2023, <https://www.atlanticcouncil.org/content-series/atlantic-council-strategy-paper-series/a-maritime-blockade-of-taiwan-by-the-peoples-republic-of-china-a-strategy-to-defeat-fear-and-coercion/>.

76 Kathleen Magramo et al., "October 11, 2022 Russia-Ukraine News," CNN, October 11, 2022, <https://edition.cnn.com/europe/live-news/russia-ukraine-war-news-10-11-22/index.html>.

recent campaign⁷⁷ attacking large-scale thermal and hydroelectric power plants illustrates the utility of dispersed energy infrastructure. Like Ukraine, Taiwan should disperse and harden its energy storage inventories to the maximal feasible extent.

Rationing plans

While both Taiwan's electricity supply *and* demand will be very hard to predict in a state of emergency, rationing plans must be considered—especially for the island's manufacturing and semiconductor industries.

Taiwan's economy is uniquely⁷⁸ tied to electricity-intensive manufacturing, as industrial consumers accounted for more than 55 percent of Taiwan's electricity consumption in 2023.⁷⁹ Most of these industrial producers (such as chip-maker Taiwan Semiconductor Manufacturing Company) service export markets—not Taiwan. While the PRC might attempt to disrupt the island's energy and electricity supply via cyber and kinetic means, Taiwan's electricity consumption would fall dramatically during a crisis if Taiwan's industries were forced to shut down. Although the closure of Taiwan's industry would prove economically ruinous, it would also make the island's electricity and energy issues much more manageable. Adding an additional layer of complication, many of Taiwan's most valuable exports – such as chips – are shipped via civilian airliners, not on seaborne vessels, and would consequently be more difficult to interdict in circumstances short of war.⁸⁰ Taiwan should prepare rationing plans for a variety of contingencies, adapting to a range of scenarios, including a quarantine, siege, or even kinetic conflict. Taiwan must be ready.

Energy recommendations for Taiwan

- Gradually raise electricity and energy prices, communicating that price hikes will persist and require significant adjustments over the medium term.
- Expand the frequency of electricity price reviews from twice a year to a quarterly basis. More frequent price adjustments will allow smaller incremental increases while also enabling Taiwan to respond more quickly to potential contingencies.
- Expand fiscal support for indigenous forms of energy. Demand-side management programs could include virtual power plants, building efficiency measures, two-way air conditioning units, and more. On the supply side, Taiwan should incentivize indigenous energy production, including nuclear energy, onshore wind, offshore wind, and solar.
- Extend the life of Taiwan's nuclear energy power plants and consider expanding capacity. Nuclear energy is not only Taiwan's best option for meeting its summer generation needs but also extremely safe and reliable. In the event of a conflict, the PRC is extremely unlikely to launch highly escalatory and provocative attacks against nuclear facilities on territory it seeks to occupy.
- Bolster domestic energy supplies and decarbonization objectives including by considering easing localization requirements for offshore wind projects—while ensuring that PRC components and sensors are not incorporated.
- Disperse and, where possible, harden energy and electricity assets and volumes across the island for both military and civil defense needs.
- Examine potential alternatives to diesel, as diesel inventories can begin to degrade after several weeks, including “long-duration diesel” solutions that, while more polluting, could extend the shelf life of its inventories, enhancing the durability of Taiwan's military and civil defense efforts.
- Deepen liquefied natural gas (LNG) ties with the United States. Contracting with US LNG producers would moderately bolster Taiwan's energy security, as the PRC would be more reluctant to interdict US cargoes than vessels from other nations.
- Conduct comprehensive studies into energy contingency planning, examining how energy and electricity would be prioritized and rationed during various scenarios.

77 Tom Balforth, “Major Russian Air Strikes Destroy Kyiv Power Plant, Damage Other Stations,” Reuters, November 2024, [https://www.reuters.com/world/europe/russian-missile-strike-targets-cities-across-ukraine-2024-04-11/#:~:text=KYIV%2C%20April%2011%20\(Reuters\),runs%20low%20on%20air%20defences](https://www.reuters.com/world/europe/russian-missile-strike-targets-cities-across-ukraine-2024-04-11/#:~:text=KYIV%2C%20April%2011%20(Reuters),runs%20low%20on%20air%20defences).

78 Global Taiwan Institute, “Taiwan's Electrical Grid and the Need for Greater System Resilience,” June 14, 2023, <https://globaltaiwan.org/2023/06/taiwans-electrical-grid-and-the-need-for-greater-system-resilience/>.

79 “3-04 Electricity Consumption (3-04 電力消費),” Taiwan Energy Statistics Monthly Report (能源統計月報), accessed May 6, 2024, <https://www.esist.org.tw/newest/monthly?tab=%E9%9B%BB%E5%8A%9B>.

80 Alperovitch, D. (2024, June 6). *A Chinese economic blockade of Taiwan would fail or launch a war*. War on the Rocks. <https://warontherocks.com/2024/06/a-chinese-economic-blockade-of-taiwan-would-fail-or-launch-a-war/>

Food and water resiliency

Taiwan's food supply needs will be significant in the event of a contingency, but pale in comparison to its energy and water requirements. Taiwan's water security is a serious concern, as it is already suffering from water access issues in noncrisis periods. Taiwan should prioritize scarce land for electricity generation, especially onshore wind and solar, which are much less water-intensive than coal and natural gas generation. Repurposing farmland for renewables would ease Taiwan's electricity and water needs in peacetime and during any crisis.

Taiwan's food security challenges are serious, but manageable. The island's self-sufficiency ratio for food stands at about 40 percent, after rising somewhat in recent years. Unlike energy, however, Taiwan can both store food, especially rice, and replenish these inventories. Meals ready to eat (MREs) can store for more than eighteen months.

Additionally, the island would likely be able to resupply itself aerially in all situations short of conflict. The PRC might well be extremely reluctant to shoot down a civilian aircraft resupplying Taiwan with food. The PRC's shutdown of a civilian aircraft would damage external perceptions of the PRC, and strengthen global support for sanctions. While there can be no certainty, the PRC's self-interest in managing perceptions of a confrontation would increase the likelihood of the safe transit of aerial and perhaps even maritime food deliveries to the island.

Taiwan's water access problems are serious. Water shortages have manifested even in peacetime, as Taiwan experienced a severe drought in 2021. During a contingency with the PRC, Beijing might attempt to exploit this vulnerability.

Luckily, Taiwan's water resiliency can be strengthened by tackling agricultural consumption and, wherever politically and technically feasible, repurposing farmland for energy generation. From 2013 to 2022, 71 percent of Taiwan's water consumption was attributable to agriculture. Meanwhile, Taiwan's industries comprised only 10 percent of demand during that period, with domestic (i.e., residential and commercial) consumption accounting for the remainder. Taiwan's water needs are growing, due to "thirsty" industrial customers, but the agricultural sector is primarily responsible for the majority of the island's consumption, although consumption and supply sources vary across the island.

Taiwan's policymakers recognize its water problems and have begun raising water prices, especially for heavy users. Taiwan should continue to encourage efficiency by gradually but perceptibly increasing water prices. Concomitantly, it should further reduce demand by repurposing water-intensive farmland for electricity generation, when feasible. Repurposing farmland will undoubtedly prove politically difficult, but it will also improve Taiwan's water and electricity resiliency.

Food and water security recommendations

- Conduct comprehensive studies of water and food security contingency planning.
- Prioritize energy and water security needs over food production.
- Secure and disperse inventories of foodstuffs, such as MREs, medicines, and water, along with water purification tablets.
- Bolster the island's cold storage supply chains and overall foodstuff inventories.
- Plan and work with partners to stage food supply if a Berlin airlift-style operation becomes necessary.
- Continue to encourage water conservation by increasing water prices gradually but steadily.
- Ensure redundancy of water supplies and systems, especially in the more populous northern part of the island.
- Ensure that drinking water and sanitation systems can operate continuously, after accounting for any electricity needs.

Sources: Gustavo F. Ferreira and J. A. Critelli, "Taiwan's Food Resiliency—or Not—in a Conflict with China," *US Army War College Quarterly: Parameters* 53, no. 2 (2023), doi:10.55540/0031-1723.3222; Joseph Webster, "Does Taiwan's Massive Reliance on Energy Imports Put Its Security at Risk?," *New Atlanticist*, Atlantic Council blog, July 7, 2023, <https://www.atlanticcouncil.org/blogs/new-atlanticist/does-taiwans-massive-reliance-on-energy-imports-put-its-security-at-risk/>; Amy Chang Chien, Mike Ives, and Billy H. C. Kwok, "Taiwan Prays for Rain and Scrambles to Save Water," *New York Times*, May 28, 2021, <https://www.nytimes.com/2021/05/28/world/asia/taiwan-drought.html>; "Water Resources Utilization," Ministry of Economic Affairs (MOEA), Water Resources Agency, 2022, <https://eng.wra.gov.tw/cp.aspx?n=5154&dn=5155>; Menghsuan Yang, "Why Did Formosa Plastics Build Its Own Desalination Facility?," *CommonWealth Magazine*, May 31, 2023, <https://english.cw.com.tw/article/article.action?id=3440>; and Chao Li-yan and Ko Lin, "Taiwan State-Owned Utility Evaluates Water Price Adjustments," *Focus Taiwan*, January 26, 2024, <https://focustaiwan.tw/society/202401260017#:~:text=As%20of%20Aug>.

Note: The Berlin airlift of 1948 and 1949 demonstrates the power of aerial food replenishment logistics in an uncontested environment. From June 26, 1948, to September 30, 1949, Allied forces delivered more than 2.3 million tons of food, fuel, and supplies to West Berlin in over 278,000 airdrops. While Taiwan's population of more than twenty-three million is significantly larger than West Berlin's population of 2.5 million, the world civilian air cargo fleet has expanded dramatically over the past seventy-five years. In all situations short of conflict, Taiwan would be able to restock food from the air. For more on the Berlin airlift, see Katie Lange, "The Berlin Airlift: What It Was, Its Importance in the Cold War," *DOD News*, June 24, 2022, <https://www.defense.gov/News/Feature-Stories/Story/Article/3072635/the-berlin-airlift-what-it-was-its-importance-in-the-cold-war/>.

Enhancing defense resilience

Ever since Beijing leveraged then-Speaker Nancy Pelosi's August 2022 visit to Taiwan as an excuse to launch large-scale joint blockade military exercises, pundits have labeled the residual military situation around Taiwan as a "new normal." Yet there is really nothing normal about a permanent presence of People's Liberation Army (PLA) Navy warships menacingly surrounding the island along its twenty-four nautical mile contiguous zone, and nothing usual about increasing numbers of manned and unmanned military aircraft crossing the tacit median line in the Taiwan Strait—a line that held significance for seven decades as a symbol of cross-strait stability. Nor should it be viewed as normal that a steady stream of high-altitude surveillance balloons—which are suspected of collecting military intelligence—violate Taiwan's airspace.⁸¹ Some have better described this "new normal" as a strategy akin to an anaconda noticeably tightening its grip around the island, drawing close enough to reduce warning time and provocative enough to raise the risk of inadvertent clashes. In other words, the PRC has unilaterally dialed up a military cost-imposition campaign meant to chip away at peace and stability across the Taiwan Strait, wear down Taiwan's military, and erode confidence and social cohesion in Taiwan society.

Russia's full-scale invasion of Ukraine in 2022 was an additional wake-up call for the citizens of Taiwan, following mainland China's 2019 crackdown on Hong Kong freedoms, heightening recognition of the risks presented by the PRC and, in particular, that the long-standing status quo in cross-strait relations is no longer acceptable to Beijing. Taiwan thus finds itself in the unenviable position of simultaneously countering PLA gray zone intrusions and cognitive warfare—what NATO calls affecting attitudes and behaviors to gain advantage⁸²—while beefing itself up militarily to deter the growing threat of a blockade or assault.

With this backdrop, Taipei authorities have since embarked on long-overdue reforms in defense affairs, marked by several developments aimed at bolstering the island

democracy's military capabilities and readiness in the face of growing threats from Beijing.

First, Taiwan's overall defense spending has undergone seven consecutive year-on-year increases, reaching 2.5 percent of gross domestic product.⁸³ While this is commendable, Taiwan's defense requirements are very substantial, and its budget in US dollars is only \$19.1 billion.⁸⁴ Accordingly, it will be important for Taiwan to continue the trend of higher defense spending to at least 3 percent of GDP both to bolster Taiwan's military capabilities and as a deterrent signal to Beijing—and also to garner international community recognition that Taiwan is serious about its own defense. A key element will be to ensure that Taiwan has sufficient stocks of ammunition and other weapons capabilities to fight effectively until the United States could fully engage and in the event of a longer war. One area that deserves a high degree of attention is defense against ballistic and cruise missiles and unmanned vehicles. Especially in light of the recent coalition success in defeating such Iranian attacks against Israel, planning should be undertaken to assure comparable success for Taiwan against PRC attacks. Adding mobile, short-range air defenses to the high-priority list of military investments for Taiwan—such as the highly mobile National Advanced Surface-to-Air Missile System (NASAMS)⁸⁵—will make it harder for the PLA to find and destroy Taiwan defenses, especially if combined with passive means for target detection and missile guidance.

Second, the new president can kick-start an enhanced approach to defense by embracing full integration of public-private innovation and adopting Ukraine's model of grass-roots innovation for defense, which has served it well through a decade of war against a much larger Russia. Recognizing that innovation is itself a form of resilience, Taiwan can draw valuable lessons from Ukraine, particularly in leveraging private-sector expertise. By implementing what some Ukrainian defense experts term a "capability accelerator" to integrate emerging technologies into mission-focused capabilities, Taiwan can enhance its resilience

81 "The Ministry of National Defense Issues a Press Release Explaining Reports That 'Airborne Balloons by the CCP Had Continuously Flown over Taiwan,'" Taiwan Ministry of National Defense, January 6, 2024, <https://www.mnd.gov.tw/english/Publish.aspx?title=News%20Channel&SelectStyle=Defense%20News%20&p=82479>.

82 "Cognitive Warfare," Allied Command Transformation, NATO, accessed May 24, 2024, <https://www.act.nato.int/activities/cognitive-warfare/#:~:text=NORFOLK%2C%20VA%20E2%80%93%20Cognitive%20Warfare%20includes,an%20advantage%20over%20an%20adversary>.

83 "Taiwan Announces an Increased Defense Budget for 2024," Global Taiwan Institute, September 20, 2023, <https://globaltaiwan.org/2023/09/taiwan-announces-an-increased-defense-budget-for-2024/>.

84 Yu Nakamura, "Taiwan Allots Record Defense Budget for 2024 to Meet China Threat," *Nikkei Asia*, August 24, 2023, <https://asia.nikkei.com/Politics/Defense/Taiwan-allots-record-defense-budget-for-2024-to-meet-China-threat>.

85 "NASAMS: National Advanced Surface-to-Air Missile System," Raytheon, accessed May 12, 2024, <https://www.rtx.com/raytheon/what-we-do/integrated-air-and-missile-defense/nasams>.

and swiftly adapt to evolving security challenges, including rapidly fielding a high volume of unmanned systems to achieve distributed surveillance, redundant command and control, and higher survivability.⁸⁶ This comprehensive approach, which recognizes the private sector as the greatest source of innovation in today's complex security environment, holds significant potential for enhancing Taiwan's defense capabilities through the utilization of disruptive technologies. The island's overall resilience would significantly benefit by drawing the private sector in as a direct stakeholder in national defense matters.

Ukraine's grass-roots model of defense innovation, spearheaded by volunteers, nongovernment organizations, and international partners, is a worthy and timely model for Taiwan. Ukraine's approach has yielded significant advancements in drone warfare, as well as sophisticated capabilities like the Delta battlefield management system—a user-friendly cloud-based situational awareness tool that provides real-time information on enemy and friendly forces through the integration of data from sources such as drones, satellites, and even civilian reports.⁸⁷ This collaborative model, reliant on cooperation between civilian developers and military end users, has propelled Ukraine's military technological revolution by integrating intelligence and surveillance tasks, while enhancing decision-making and kill-chain target acquisition. Taiwan will benefit from a comparable approach.

Third, as suggested above, Taiwan should focus a large portion of its defense budget on low-cost, highly effective systems. In terms of force structure, it appears that Taiwan has settled on a design that blends large legacy platforms of a twentieth-century military with the introduction of more survivable and distributable low-end asymmetric capabilities. The latter are best exemplified by Taiwan's indigenously produced *Ta Chiang*-class of high-speed, guided-missile corvettes (PGG) and *Min Jiang*-class fast mine laying boats (FMLB).⁸⁸ But much more must be done to bolster Taiwan's overall defense capabilities by focusing on less expensive, but nonetheless highly effective systems.

In Ukraine's battle against Russian Federation invaders, drones have provided Ukrainian forces with important tactical capabilities by enabling them to gather intelligence, monitor enemy movements, and conduct precision strikes on high-value targets. Taiwan can comparably utilize low-cost UAVs to establish mesh networks that connect devices for intelligence, surveillance, and reconnaissance and for targeting that would be invaluable in countering a PRC amphibious assault. Lessons from Ukraine further highlight the importance of having the right mix of drone types and capabilities in *substantial* stockpiles, capable of a variety of missions. Notably, Ukrainian officials have called for the production of more than one million domestically produced drones in 2024.⁸⁹ Then-President Tsai's formation of a civilian-led "drone national team" program is a commendable step in this direction and underscores the power of collaborative innovation in joint efforts between users.⁹⁰ Encouraging cooperation between Taiwan drone makers and US private industry will accelerate the development of a combat-ready unmanned systems fleet with sufficient range, endurance, and payload to enhance situational awareness and battlefield effects.

Concurrent with those efforts utilizing unmanned systems, Taiwan should bolster its naval mining capabilities as a strategic measure against PRC aggression. Naval mines represent one of the most cost-effective and immediately impactful layers of defense.⁹¹ In this regard, Taiwan's new *Min Jiang* class of FMLB represents the right type of investments in capabilities which could prove pivotal in thwarting potential invasion attempts.

Even more significantly for a Taiwan audience, Ukraine broke a blockade of its Black Sea ports using a combination of naval drones and coastal defense missiles—and repelled the once-mighty Russian Black Sea Fleet—all without a traditional navy of its own.⁹² Faced with clear intent by a PLA Navy practicing daily to isolate the island, the time is past due for Taiwanese authorities to hone their own counterblockade skills including a heavy reliance on unmanned surface vehicles.

86 Lopatin, "Bind Ukraine's Military-Technology Revolution."

87 Grace Jones, Janet Egan, and Eric Rosenbach, "Advancing in Adversity: Ukraine's Battlefield Technologies and Lessons for the U.S.," Policy Brief, Belfer Center for Science and International Affairs, Harvard Kennedy School, July 31, 2023, <https://www.belfercenter.org/publication/advancing-adversity-ukraines-battlefield-technologies-and-lessons-us>.

88 For more information, see, e.g., Peter Suci, "Future of Taiwan's Navy: Inside the Tuo Chiang-Class Missile Corvettes," *National Interest*, March 27, 2024, <https://nationalinterest.org/blog/buzz/future-taiwans-navy-inside-tuo-chiang-class-missile-corvettes-210269>; and Xavier Vavasour, "Taiwan Launches 1st Mine Laying Ship for ROC Navy," *Naval News*, August 5, 2020, <https://www.navalnews.com/naval-news/2020/08/taiwan-launches-1st-mine-laying-ship-for-roc-navy/>.

89 Mykola Bielyskov, "Outgunned Ukraine Bets on Drones as Russian Invasion Enters Third Year," *Ukraine Alert*, Atlantic Council blog, February 20, 2024, <https://www.atlanticcouncil.org/blogs/ukrainealert/outgunned-ukraine-bets-on-drones-as-russian-invasion-enters-third-year/>.

90 Yimou Lee, James Pomfret, and David Lague, "Inspired by Ukraine War, Taiwan Launches Drone Blitz to Counter China," Reuters, July 21, 2023, <https://www.reuters.com/investigates/special-report/us-china-tech-taiwan/>.

91 Franklin D. Kramer and Lt. Col. Matthew R. Crouch, *Transformative Priorities for National Defense*, Scowcroft Center for Strategy and Security, Atlantic Council, 2021, <https://www.atlanticcouncil.org/wp-content/uploads/2021/06/Transformative-Priorities-Report-2021.pdf>.

92 Peter Dickinson, "Ukraine's Black Sea Success Exposes Folly of West's 'Don't Escalate' Mantra," *Ukraine Alert*, Atlantic Council, January 22, 2024, <https://www.atlanticcouncil.org/blogs/ukrainealert/ukraines-black-sea-success-provides-a-blueprint-for-victory-over-putin/>.

Taiwan should also make rapid investments in port infrastructure and defenses along Taiwan's eastern seaboard in places such as Su'ao and Hualien harbors, which can serve as deepwater ports that are accessible, strategic, antiblockade strongpoints, and where any conceivable PLA blockade would be at its weakest and most vulnerable point logistically. Su'ao harbor, as a potential future homeport for Taiwan's new indigenous *Hai Kun*-class diesel submarines, could also serve a dual purpose as an experimentation and development zone for public-private collaboration on unmanned-systems employment and operations. Infrastructure investments in East Coast ports could enhance the island's ability to attain emergency resupply of energy, food, humanitarian supplies, and munitions under all conditions, broadening options for international community aid and complicating PLA efforts.

Fourth, every new capability needs trained operators who are empowered to employ and engage. This year Taiwan began implementation of a new, one-year conscript training system for male adults born after January 1, 2005 (up from a wholly inadequate four months of conscription in the past decade).⁹³ Taiwan's "all-out defense" plan realigns into a frontline main battle force consisting of all-volunteer career military personnel, backed up by a standing garrison force composed mainly of conscripted military personnel guarding infrastructure, along with a civil defense system integrated with local governments and private-sector resources. Upon mobilization, there would also be a reserve force to supplement the main battle and garrison forces.

According to details laid out in its 2023 National Defense Report, Taiwan's revamped one-year conscript system and reorganized reserve mobilization system place significant emphasis on traditional military combat skills, such as rifle marksmanship and operation of mortars.⁹⁴ However, in response to evolving security challenges and the changing nature of warfare, Taiwan's military should incorporate greater training in emerging technologies and unconventional tactics, along with decentralized command and control, especially in the areas of drone warfare, where unmanned aerial vehicles and surface vessels play a crucial role in reconnaissance, surveillance, and targeted

strikes. By integrating drone warfare training into the conscript system as well as in annual reserve call-up training, Taiwan can better prepare its military personnel to adapt to modern battlefield environments and effectively counter emerging threats.

Integrating drone operations into military operations down to the conscript and reservist level offers a cost-effective means to enhance battlefield situational awareness and operational capabilities, and also has the added benefit of enhancing the attractiveness and value of a mandatory conscription system emerging from years of low morale and characterized by Taiwan's outgoing president as "insufficient" and "full of outmoded training."⁹⁵ Recognizing the imperative to modernize military training to face up to a rapidly expanding PLA threat, Taiwan's military force realignment plan came with a promise to "include training in the use of Stinger missiles, Javelin missiles, Kestrel rockets, drones, and other new types of weapons . . . in accordance with mission requirements to meet the needs of modern warfare."⁹⁶ Looking at the example of Ukraine, where drones have been utilized, underscores the importance of incorporating drone warfare training into its asymmetric strategy.

The Taiwan Enhanced Resilience Act "prioritize[d] realistic training" by the United States, with Taiwan authorizing "an enduring rotational United States military presence that assists Taiwan in maintaining force readiness."⁹⁷ There have been numerous reports of US special forces in Taiwan,⁹⁸ and those forces could provide training in tactical air control, dynamic targeting, urban warfare, and comparable capabilities.⁹⁹ Likewise, parts of an Army Security Force Assistance Brigade could do similar work on a rotational basis, on- or off-island.

To facilitate a comprehensive and integrated approach to defense planning and preparedness between the military, government agencies, and civilian organizations, Taiwan has also established the All-out Defense Mobilization Agency, which (as noted above) is a centralized body subordinate to the Ministry of National Defense that is tasked with coordinating efforts across various sectors, down to the local level, to enhance national defense readiness. That agency would be significantly more effective if raised

93 Ministry of National Defense, *ROC National Security Defense Report 2023*, <https://www.mnd.gov.tw/newupload/ndr/112/112ndreng.pdf>.

94 Ministry of National Defense, *ROC National Security Defense Report 2023*.

95 "President Tsai Announces Military Force Realignment Plan," Office of the President, December 27, 2022, <https://english.president.gov.tw/NEWS/6417>.

96 "President Tsai Announces Military Force Realignment Plan."

97 International Military Education and Training Cooperation with Taiwan, 22 U.S.C. § 3353 (2022), <https://www.law.cornell.edu/uscode/text/22/3353>.

98 Guy D. McCardl, "US Army Special Forces to Be Deployed on Taiwanese Island Six Miles from Mainland China," SOFREP, March 8, 2024, <https://sofrep.com/news/us-army-special-forces-to-be-deployed-on-taiwanese-island-six-miles-from-mainland-china/>.

99 "Taiwan Defense Issues for Congress," Congressional Research Service, CRS Report R48044, updated May 10, 2024, <https://crsreports.congress.gov/product/pdf/R/R48044>.

to the national level with a broadened mandate as part of a comprehensive approach.

The Taiwanese leadership also should consider elevating their efforts to create a large-scale civil defense force, offering practical skills training which would appeal to Taiwanese willing to dedicate time and effort toward defense of their communities and localities. These skills could include emergency medical training, casualty evacuation, additive manufacturing, drone flying, and open-source intelligence. Private, nonprofit civil defense organizations such as Taiwan's Kuma Academy hold widespread appeal to citizens seeking to enhance basic preparedness skills.¹⁰⁰ With a curriculum that covers topics ranging from basic first aid to cognitive warfare, Kuma Academy's popular classes typically sell out within minutes of going online. According to a recent survey of domestic Taiwan opinions sponsored by Spirit of America, "When facing external threats, 75.3% of the people agree that Taiwanese citizens have an obligation to defend Taiwan."¹⁰¹ A well-trained civil defense force and other whole-of-society resilience measures provide an additional layer of defense and enhance social cohesion to better deny Beijing's ultimate political objective of subjugating the will of the people.

Defense resilience recommendations for Taiwan

- Raise defense spending to at least 3 percent of GDP.
- Adopt Ukraine's model of grass-roots innovation in defense.
- Focus a large portion of its defense budget on low-cost, highly effective systems including unmanned vehicles and naval mines.
- Incorporate greater training in emerging technologies and unconventional tactics for conscripts and reserves.
- Invest in East Coast port infrastructure as counter-blockade strongholds.
- Elevate the All-out Defense Mobilization Agency to the national level and implement a larger civil defense force that fully integrates civilian agencies and local governments.

¹⁰⁰ Jordyn Haime, "NGOs Try to Bridge Taiwan's Civil Defense Gap," China Project, August 4, 2023, <https://thechinaproject.com/2023/08/04/ngos-try-to-bridge-taiwans-civil-defense-gap/>.

¹⁰¹ Spirit of America, Taiwan Civic Engagement Survey, January 2024.

Conclusion

On April 3, 2024, Taiwan was struck by the strongest earthquake in twenty-five years. In the face of this magnitude 7.4 quake, Taiwan’s response highlights the effectiveness of robust investment in stricter building codes, earthquake alert systems, and resilience policies, resulting in minimal casualties and low infrastructure damage.¹⁰² Taiwan’s precarious position on the seismically vulnerable Ring of Fire, a belt of volcanoes around the Pacific Ocean, mirrors its vulnerability under constant threat of military and gray zone aggression from a mainland China seeking seismic changes in

geopolitical power. Drawing from its success in preparing for and mitigating the impact of natural disasters, Taiwan can apply a similarly proactive approach in its defense preparedness. Safeguarding Taiwan’s sovereignty and security requires investments in a comprehensive security strategy for resilience across society—including cybersecurity for critical infrastructures, bolstering energy security, and enhanced defense resilience. Such an approach would provide Taiwan the greatest likelihood of deterring or, if necessary, defeating PRC aggression including through blockade or kinetic conflict.

¹⁰² Amy Hawkins and Chi Hui Lin, “As Well Prepared as They Could Be’: How Taiwan Kept Death Toll Low in Massive Earthquake,” *Observer*, April 7, 2024, <https://www.theguardian.com/world/2024/apr/07/as-well-prepared-as-they-could-be-how-taiwan-kept-death-toll-low-in-massive-earthquake>.

About the authors



Franklin D. Kramer is a distinguished fellow at the Atlantic Council and a member of its board. He is a former US assistant secretary of defense for international security affairs.



Philip Yu is a nonresident senior fellow in the Indo-Pacific Security Initiative at the Atlantic Council's Scowcroft Center for Strategy and Security, and a retired US Navy rear admiral.



Joseph Webster is a senior fellow at the Atlantic Council's Global Energy Center, a nonresident senior fellow in the Indo-Pacific Security Initiative at the Atlantic Council's Scowcroft Center for Strategy and Security, and editor of the independent *China-Russia Report*.



Elizabeth "Beth" Sizeland is a nonresident senior fellow at the Scowcroft Strategy Initiative of the Atlantic Council's Scowcroft Center for Strategy and Security. Earlier, she served in the United Kingdom's government including as deputy national security adviser and as adviser to the UK prime minister on intelligence, security, and resilience issues.

This analysis reflects the personal opinions of the authors.

Acknowledgements

The authors would like to thank the following individuals for their helpful comments and feedback:

Amber Lin • Elsie Hung • Kwangyin Liu • Alison O’Neil



CHAIRMAN

*John F.W. Rogers

EXECUTIVE CHAIRMAN EMERITUS

*James L. Jones

PRESIDENT AND CEO

*Frederick Kempe

EXECUTIVE VICE CHAIRS

*Adrienne Arsht

*Stephen J. Hadley

VICE CHAIRS

*Robert J. Abernethy

*Alexander V. Mirtchev

TREASURER

*George Lund

DIRECTORS

Stephen Achilles

Elliot Ackerman

*Gina F. Adams

Timothy D. Adams

*Michael Andersson

Alain Bejjani

Colleen Bell

Sarah E. Beshar

Karan Bhatia

Stephen Biegun

Linden P. Blue

Brad Bondi

John Bonsell

Philip M. Breedlove

David L. Caplan

Samantha A. Carl-Yoder

*Teresa Carlson

*James E. Cartwright

John E. Chapoton

Ahmed Charai

Melanie Chen

Michael Chertoff

*George Chopivsky

Wesley K. Clark

*Helima Croft

Ankit N. Desai

Dario Deste

*Lawrence Di Rita

*Paula J. Dobriansky

Joseph F. Dunford, Jr.

Richard Edelman

Stuart E. Eizenstat

Tara Engel

Mark T. Esper

Christopher W.K. Fetzer

*Michael Fisch

Alan H. Fleischmann

Jendayi E. Frazer

*Meg Gentle

Thomas H. Glocer

John B. Goodman

Sherri W. Goodman

Marcel Grisnigt

Jarosław Grzesiak

Murathan Günal

Michael V. Hayden

Tim Holt

*Karl V. Hopkins

Kay Bailey Hutchison

Ian Ilnatowycz

Wolfgang F. Ischinger

Deborah Lee James

*Joia M. Johnson

*Safi Kalo

Andre Kelleners

Brian L. Kelly

John E. Klein

*C. Jeffrey Knittel

Joseph Konzelmann

Keith J. Krach

Franklin D. Kramer

Laura Lane

Almar Latour

Yann Le Pallec

Jan M. Lodal

Douglas Lute

Jane Holl Lute

William J. Lynn

Mark Machin

Marco Margheri

Michael Margolis

Chris Marlin

William Marron

Roger R. Martella Jr.

Gerardo Mato

Erin McGrain

John M. McHugh

*Judith A. Miller

Dariusz Mioduski

*Richard Morningstar

Georgette Mosbacher

Majida Mourad

Virginia A. Mulberger

Mary Claire Murphy

Julia Nesheiwat

Edward J. Newberry

Franco Nuschese

Joseph S. Nye

*Ahmet M. Ören

Ana I. Palacio

*Kostas Pantazopoulos

Alan Pellegrini

David H. Petraeus

Elizabeth Frost Pierson

*Lisa Pollina

Daniel B. Poneman

Robert Portman

*Dina H. Powell

McCormick

Michael Punke

Ashraf Qazi

Thomas J. Ridge

Gary Rieschel

Charles O. Rossotti

Harry Sachinis

C. Michael Scaparrotti

Ivan A. Schlager

Rajiv Shah

Wendy R. Sherman

Gregg Sherrill

Jeff Shockey

Kris Singh

Varun Sivaram

Walter Slocombe

Christopher Smith

Clifford M. Sobel

Michael S. Steele

Richard J.A. Steele

Mary Streett

Nader Tavakoli

*Gil Tenzer

*Frances F. Townsend

Clyde C. Tuggle

Francesco G. Valente

Melanne Verveer

Tyson Voelkel

Kemba Walden

Michael F. Walsh

Ronald Weiser

*Al Williams

Ben Wilson

Maciej Witucki

Neal S. Wolin

Tod D. Wolters

*Jenny Wood

Alan Yang

Guang Yang

Mary C. Yates

Dov S. Zakheim

HONORARY DIRECTORS

James A. Baker, III

Robert M. Gates

James N. Mattis

Michael G. Mullen

Leon E. Panetta

William J. Perry

Condoleezza Rice

Horst Teltschik

William H. Webster

**Executive Committee Members*

List as of April 24, 2024



The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

© 2024 The Atlantic Council of the United States. All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means without permission in writing from the Atlantic Council, except in the case of brief quotations in news articles, critical articles, or reviews. Please direct inquiries to:

Atlantic Council

1030 15th Street, NW, 12th Floor, Washington, DC 20005

(202) 463-7226, www.AtlanticCouncil.org